ThinkVantage

Client Security Solution 8.3
デプロイメント・ガイド

日付: 2009年10月28日

ThinkVantage 指紋認証ソフトウェア 5.9.2 および Lenovo Fingerprint Software 3.3 を含む

ThinkVantage

Client Security Solution 8.3
デプロイメント・ガイド

日付: 2009年10月28日

目次

まえがき

本書に記載されている情報は、ThinkVantage® Client Security Solution および指紋認証ソフトウェアがインストールされている Lenovo® コンピューターを対象としています。

Client Security Solution と指紋認証ソフトウェアの目的は、クライアント・データを保護することによってお客様のシステムを保護し、セキュリティー・ブリーチ (抜け穴) を犯そうとする試みを食い止めることです。

「*Client Security Solution デプロイメント・ガイド*」では、1 台以上のコンピューターに Client Security Solution および指紋認証ソフトウェアをインストールするために必要な情報と、IT および会社の方針をサポートするためにカスタマイズ可能な管理機能ツールについての説明やシナリオが記載されています。

本書は、IT 管理者、または ThinkVantage Client Security Solution および指紋認証ソフトウェアを組織内の PC にデプロイする担当者を対象としています。ご提案またはコメントは、Lenovo 認定担当者にご連絡ください。本書は定期的に更新されます。最新の資料については以下の Lenovo Web サイトで確認できます。
http://www-307.ibm.com/pc/support/site.wss/TVAN-ADMIN.html

Client Security Solution および指紋認証ソフトウェアのワークスペースに組み込まれているさまざまなコンポーネントの使用に関する質問および情報は、Client Security Solution および指紋認証ソフトウェアに付属のオンライン・ヘルプ・システムおよびユーザー・ガイドを参照してください。

第 1 章 概要

本章では、Client Security Solution および指紋認証ソフトウェアの概要を示します。本デプロイメント・ガイドで説明されているテクノロジーは、PC の使い勝手と自己完結性を向上させ、展開を促進し単純化する強力なツールを提供するので、IT プロフェッショナルの方に大きなメリットをもたらします。 ThinkVantage テクノロジーの支援により、IT プロフェッショナルの方は、個別の PC の問題を解決する時間を短縮できるので、本来の作業に多くの時間を費やすことができるようになります。

Client Security Solution

Client Security Solution ソフトウェアの第一の目的は、お客様が資産としての PC を保護し、PC 上の機密データを保護し、さらに PC がアクセスするネットワーク接続を保護することを補助することです。 (TCG (Trusted Computing Group) という業界団体が仕様を定めている TPM (Trusted Platform Module) を含む Lenovo システムの場合、Client Security Solution ソフトウェアは、システムのトラステッド・ルートとしてハードウェアを活用します。システムにエンベデッド・セキュリティー・チップが含まれていない場合、Client Security Solution は、システムの信頼のルートとしてソフトウェア・ベースの暗号化鍵を活用します。)

Client Security Solution 8.3 には、以下の機能が含まれています。

- **Windows® パスワードまたは Client Security Solution パスフレーズによるユーザー認証の保護**

  Client Security Solution は、認証の際にユーザーの Windows パスワードまたは Client Security Solution パスフレーズを受け入れるように構成できます。Windows パスワードの場合は Windows を使用するため、便利で管理が容易です。Client Security Solution パスフレーズではセキュリティーが強化されます。どちらの認証方式を使用するかは管理者が選択でき、この設定はユーザーが Client Security Solution に登録した後でも変更することが可能です。

- **指紋によるユーザー認証**

  内蔵、または USB 接続の指紋センサーを活用し、パスワードで保護されたアプリケーションに対してユーザーを認証します。

- **スマート・カードによるユーザー認証**

  ユーザー認証に登録済みのスマート・カードを活用します。

- **多層のユーザー認証による Windows ログオンおよびさまざまな Client Security Solution 操作**

  さまざまなセキュリティー関連操作に対して複数の認証装置 (Windows パスワード/Client Security パスフレーズ、指紋、およびスマート・カード) を定義します。

- **パスワード管理**

  ユーザー ID やパスワードなどの重要なログオン情報を安全に管理し、保存します。

- **パスワード/パスフレーズの復元**

  パスワードおよびパスフレーズの復元を利用して、Windows パスワードまたは Client Security Solution パスフレーズを忘れた場合でも、事前に構成されたセキュリティーの質問に答えることにより、Windows にログインし、Client Security Solution クレデンシャルにアクセスすることができます。

- **セキュリティー設定の監査**

  ユーザーが、詳細なワークステーション・セキュリティー設定のリストを表示し、定義された規格に準拠するように変更できるようにします。

- **ディジタル証明書の転送**

  Client Security Solution は、ユーザーとマシンの証明書の秘密鍵を保護します。Client Security Solution を使用することにより、既存の証明書の秘密鍵が保護されます。

- **認証のポリシー管理**

  管理者は、Windows ログオン、Password Manager、および証明書の操作といったアクションの場合、認証にどの装置 (Windows パスワード、Client Security Solution パスフレーズ、指紋、またはスマート・カード) が必要かを選択することができます。

Client Security Solution パスフレーズ

Client Security Solution パスフレーズは、Client Security Solution に拡張セキュリティーを提供する、ユーザー認証のオプション機能です。 Client Security Solution パスフレーズの要件は、以下のとおりです。

- 8 文字以上の長さ
- 数字が 1 文字以上入っていること
- 最近の 3 回のパスフレーズと異なること
- 反復文字は 2 文字以内
- 先頭に数字を使用しない
- 末尾に数字を使用しない
- ユーザー ID を含めない
- 現在のパスフレーズを設定してから 3 日以内は変更しない
- 現在のパスフレーズと同一の文字を連続して 3 文字以上使用しない
- Windows パスワードと異なる

Client Security Solution パスフレーズを知っているのは個々のユーザーだけであり、Client Security Solution パスフレーズを忘れた場合に復元する唯一の方法は、 Client Security Solution パスワード復元機能の活用です。ユーザーが復元のための質問に対する回答を忘れてしまった場合、Client Security Solution パスフレーズで保護されたデータを復元する方法はありません。

Client Security パスワードの復元

このオプション機能を使用すると、登録された Client Security ユーザーは、Windows パスワードや Client Security パスフレーズを忘れた場合に、3 つの質問に正しく答えることにより、復元することができます。この機能が有効である場合、ユーザーは、10 の質問の中から 3 つを選択し、それぞれの質問に対する回答を入力します。ユーザーが Windows パスワードや Client Security パスフレーズを忘れた場合は、これら 3 つの質問に回答して、そのパスワードやパスフレーズを自分でリセットするというオプションが用意されています。

注:

1. Client Security パスフレーズを使用する場合、Client Security パスワードの復元機能は忘れたパスフレーズを復元するための唯一のオプションです。ユーザーは、それら 3 つの質問に対する回答を忘れた場合、登録ウィザードを再実行しなくてはならず、前の Client Security 保護データはすべて失われます。
2. Client Security を使用して Rescue and Recovery® ワークスペースを保護する場合、「パスワード復元」オプションによって、ユーザーの Client Security パスフレーズおよび/または Windows パスワードが実際に表示されます。パスフレーズまたはパスワードが表示されるのは、Rescue and Recovery ワークスペースが Windows パスワードの変更を自動的に実行する機能を持たないためです。ワイヤレス (ネットワークに接続されていないローカル・キャッシュ・ドメイン) ユーザーが Windows ログオンでこの機能を実行する場合にも、パスフレーズまたはパスワードが表示されます。

Client Security Password Manager

Client Security Password Manager を使用すると、ユーザー ID、パスワード、およびその他の個人情報などの、忘れやすいアプリケーションや Web サイトの情報を管理することができます。 Client Security Password Manager は、ユーザーのアプリケーションや Web サイトへのアクセス全体がセキュアに保たれるように、Client Security Solution によってユーザーの個人情報を保護します。また、Client Security Password Manager プログラムでは、1 つのパスワードまたはパスフレーズを覚えておくか、指紋またはスマート・カードを使用すればよいため、時間と労力が節約されます。

Client Security Password Manager を使用すると、以下の機能を実行できます。

- **Client Security Solution ソフトウェアによるすべての保存情報の暗号化**

  Client Security Solution によってユーザーのすべての情報が自動的に暗号化されます。これにより、重要なパスワード情報が、Client Security Solution 暗号化鍵によって保護されます。

- **ユーザー ID とパスワードの自動入力**

  アプリケーションまたは Web サイトにアクセスする際に、ログイン・プロセスを自動化します。ログオン情報が Client Security Password Manager に入力されている場合は、Client Security Password Manager が自動的に必須フィールドへの記入を行い、Web サイトまたはアプリケーションに実行依頼します。

- **Client Security Password Manager インターフェースを使用した項目の編集**

  アカウント項目を編集し、すべてのオプション機能を 1 つの使いやすいインターフェースにセットアップすることができます。このインターフェースにより、パスワードと個人情報の管理を迅速かつ容易に行えるようになります。ただし、変更に関連する項目のほとんどは Client Security Password Manager が自動的に検出できるため、ユーザーはさらに簡単に項目を更新できます。

- **追加ステップを必要としない情報の保存**

  Client Security Password Manager は、重要情報が特定の Web サイトまたはアプリケーションに送信されると、それを自動的に検出できます。重要情報を検出すると、Client Security Password Manager はユーザーにプロンプトを出して情報を保存するように促し、重要情報の保存プロセスを単純化します。

- **セキュア・スクラッチ・パッドへの情報の保存**

  Client Security Password Manager を使用して、ユーザーはテキスト・データをセキュア・スクラッチ・パッドに保存することができます。ユーザーのセキュア・スクラッチ・パッドは、他の Web サイトやアプリケーションの項目と同じレベルのセキュリティーで保護できます。

- **ログイン情報のエクスポートとインポート**

  重要な個人情報をエクスポートして、その情報を PC 間で安全に移動させることができます。 Client Security Password Manager からログイン情報をエクスポートすると、パスワードで保護されたエクスポート・ファイルが作成されます。このファイルは、リムーバブル・メディアに保存することができます。このファイルを使用して、あらゆる場所でユーザーの個人情報にアクセスしたり、Client Security Password Manager を使用して項目を別の PC にインポートします。

  注:

  – Client Security Solution バージョン 7.0 および 8.*x* のエクスポート・ファイルのインポートは完全にサポートされています。Client Security Solution バージョン 6.0 の場合は、インポートが限定的にサポートされています (アプリケーション項目はインポートされません)。Client Security Software Solution バージョン 5.4*x* およびこれ以前のバージョンは、Client Security Solution バージョン 8.*x* Password Manager にインポートされません。

Security Advisor

Security Advisor を使用すると、現在 PC に設定されているセキュリティー設定の要約を表示できます。これらの設定値を使用して、現在のセキュリティー状況を表示したり、システム・セキュリティーを強化することができます。表示されるカテゴリーのデフォルト値は、Windows レジストリーによって変更できます。以下に、セキュリティー・カテゴリーの一例を示します。

- ハードウェア・パスワード
- Windows ユーザー・パスワード
- Windows パスワード・ポリシー
- 保護スクリーン・セーバー
- ファイル共有

証明書転送ウィザード

Client Security の証明書転送ウィザードは、ソフトウェア・ベースの Microsoft® 暗号サービス・プロバイダーからハードウェア・ベースの Client Security Solution CSP に、証明書に関連した秘密鍵を転送するすべてのプロセスをガイドします。転送が行われた後は、秘密鍵が Client Security Solution によって保護されるため、証明書を使用する操作はよりセキュアになります。

ハードウェア・パスワードのリセット

このツールは、Windows から独立して稼動するセキュアな環境を作成し、忘れてしまったパワーオン・パスワードやハードディスク・パスワードをリセットする際に役立ちます。 ID は、自分で作成した一連の質問に回答することによって設定されます。パスワードを忘れる前に、このセキュアな環境をできるだけ早く作成してください。登録後、ハードディスク上にこのセキュアな環境を作成するまでは、忘れてしまったハードウェア・パスワードをリセットすることはできません。このツールは、一部の PC を選択した場合のみ、使用可能です。

TPM のないシステムのサポート

Client Security Solution 8.3 は現在、対応するエンベデッド・セキュリティー・チップのない Lenovo システムをサポートしています。このサポートにより、一貫したセキュアな環境を作成するために、全社的な標準インストールを行うことが可能になります。エンベデッド・セキュリティー・チップのあるシステムはアタックに対してより堅固ですが、エンベデッド・セキュリティー・チップのないシステムの場合、Client Security Solution はソフトウェア・ベースの暗号鍵をシステムの信頼性の基盤として活用します。また、追加のセキュリティーと機能もシステムにとって有益です。

指紋認証ソフトウェア

Lenovo が提案する指紋センサーの目的は、パスワードの管理に関連したコストの削減やシステムに対するセキュリティーの強化においてお客様を補助し、お客様が規制に対応できるようにすることです。 Lenovo 社の指紋センサーとともに、指紋認証ソフトウェアを使用すると、個々の PC およびネットワークでの指紋認証が可能になります。Client Security Solution 8.3 と結合された指紋認証ソフトウェアは、拡張機能を提供します。Client Security Solution 8.3 では、ThinkVantage 指紋認証ソフトウェア 5.9.2 と Lenovo Fingerprint Software 3.3 の両方がサポートされます。これらはどちらもさまざまなマシン・タイプで使用可能です。Lenovo Web サイトで Lenovo 指紋センサーの詳細を調べたり、指紋認証ソフトウェアをダウンロードしたりすることができます。

指紋認証ソフトウェアは、以下の機能を提供します。

- **Client Security Software の機能**
  - **Microsoft Windows パスワードの置換:**

    パスワードをお客様の指紋に置き換えて、容易で高速、かつ安全なシステム・アクセスを提供します。

- **BIOS パスワード (パワーオン・パスワードとも呼ばれます) およびハードディスク・パスワードの置換:**

  パスワードをお客様の指紋と置き換えて、ログオン・セキュリティーと利便性を高めます。
- **SafeGuard Easy でドライブ全体を暗号化するための起動前指紋認証**:

  指紋認証を使用して、Windows の起動前にハードディスクを暗号化解除します。
- **BIOS および Windows へのシングル・スワイプ・アクセス:**

  起動時に指紋をセンサーに読み込ませるだけで、BIOS と Windows にアクセスすることができるので、貴重な時間を節約することができます。
- **Client Security Solution との統合:** Client Security Solution Password Manager と併用して、TPM を活用します。ユーザーは、指紋センサーに読み込ませて Web サイトにアクセスし、アプリケーションを選択します。

- **管理者機能**
  - **セキュリティー・モードの切り替え:**

    管理者は、保護モードと簡易モードを切り替えて、制限ユーザーのアクセス権限を変更することができます。
- **セキュリティー機能**
  - **ソフトウェア・セキュリティー:**

    システムに保存する際や、読み取り装置からソフトウェアに転送する際に、強い暗号化により、ユーザー・テンプレートを保護します。
  - **ハードウェア・セキュリティー:**

    セキュリティー読み取り装置には、指紋テンプレート、BIOS パスワード、および暗号鍵を保存し保護するコプロセッサーがあります。

第 2 章 インストール

本章では、Client Security Solution および指紋認証ソフトウェアをインストールする手順について説明します。Client Security Solution または指紋認証ソフトウェアをインストールする前に、インストールするアプリケーションのアーキテクチャーを理解する必要があります。本章では、各アプリケーションのアーキテクチャー、およびすべてのプログラムをインストールする前に必要な追加情報について説明します。

Client Security Solution

Client Security Solution のインストール・パッケージは、InstallShield 10.5 Premier によって Basic MSI プロジェクトとして開発されました。InstallShield は、Windows インストーラーを使用してアプリケーションをインストールします。これにより、管理者には、コマンド・ラインからのプロパティ値の設定などの、インストールをカスタマイズする多くの機能が提供されます。この章では、Client Security Solution セットアップ・パッケージの使用および実行方法について説明します。より正しく理解するために、パッケージのインストールを開始するために、章全体をお読みください。

注: これらのパッケージをインストールする場合、Lenovo Web サイトの Client Security Solution README ファイルを参照してください。README ファイルには、ソフトウェア・バージョン、サポートされるシステム、システム要件、およびインストールに役立つその他の考慮事項に関する最新の情報が含まれています。

インストール要件

このセクションでは、Client Security Solution パッケージをインストールするためのシステム要件を説明します。最良の結果を得るために、次の Web サイトにアクセスして、ソフトウェアが最新版であることを確認してください。
http://www.lenovo.com/support

Client Security Solution をインストールするには、Lenovo PC が次の要件を満たしているか、それ以上であることが必要です。

- オペレーティング・システム: Windows 7
- メモリー: 256 MB 以上推奨
  - 共用メモリー設定の場合、共用メモリーの BIOS 設定を 8 MB 以上に設定する必要があります。
  - 非共用メモリー設定の場合、非共用メモリーは 120 MB 以上必要です。
- Internet Explorer® 5.5 以上がインストールされていなければなりません。
- ハードディスク・ドライブ空き容量 300 MB。
- 解像度 800 x 600 および 24 ビット・カラーをサポートする VGA 対応ビデオ。
- ユーザーは Client Security Solution をインストールするための管理者権限を持っている必要があります。

注: Windows Server® 2003 への Client Security Solution インストール・パッケージのデプロイはサポートされていません。ただし、Windows Server 2003 からの証明書の要求はサポートしています。 80 ページの『TPM での鍵生成を使用した証明書の生成』を参照してください。

カスタム・パブリック・プロパティ

Client Security Software プログラムのインストール・パッケージには、インストールの実行時にコマンド・ラインで設定できる、一連のカスタムパブリック・プロパティが含まれています。次の表に、Windows オペレーティング・システムのカスタム・パブリック・プロパティを示します。

表 1. パブリック・プロパティ

プロパティ	説明
EMULATIONMODE	TPM が存在する場合でも、強制的にエミュレーション・モードでインストールを実行するように指定します。エミュレーション・モードでインストールするには、コマンド・ラインで EMULATIONMODE=1 と設定します。
HALTIFTPMDISABLED	TPM が使用不可状態で、インストールがサイレント・モードで実行されている場合、デフォルトではインストールをエミュレーション・モードで進めます。インストールをサイレント・モードで実行するときは、HALTIFTPMDISABLED=1 プロパティを使用して、 TPM が使用不可の場合にインストールを停止します。
NOCSSWIZARD	Client Security Solution のインストール後に Client Security Solution 登録ダイアログが自動的に表示されないようにするには、コマンド・ラインで NOCSSWIZARD=1 を設定します。このプロパティは、Client Security Solution はインストールしても、システムの構成は後でスクリプトを使用して行う管理者のために構成されています。
CSS_CONFIG_SCRIPT	ユーザーがインストールを完了し、再起動した後に構成ファイルを実行するには、CSS_CONFIG_SCRIPT="*filename*" または "*filename password*" を設定します。

表 1. パブリック・プロパティ (続き)

プロパティ	説明
SUPERVISORPW	コマンド・ラインで SUPERVISORPW=”*password*” と設定すると、スーパーバイザー・パスワードが提供され、サイレント・インストール・モードでも非サイレント・インストール・モードでも、チップが使用可能になります。チップが使用不可で、インストールをサイレント・モードで実行する場合、チップを使用可能にするには正しいスーパーバイザー・パスワードを入力する必要があります。パスワードが正しくないと、チップは使用可能になりません。
PWMGRMODE	Password Manager のみをインストールするには、コマンド・ラインで PWMGRMODE=1 と設定します。
NOSTARTMENU	「スタート」メニューにショートカットが生成されないようにするには、コマンド・ラインで NOSTARTMENU=1 と設定します。
CREATESHORTCUT	項目を「**スタート**」メニューに追加するには、コマンド・ラインで CREATESHORTCUT=1 と設定します。

TPM (Trusted Platform Module) のサポート

Client Security Solution バージョン 8.3 では、PC のエンベデッド・セキュリティー・チップである TPM (Trusted Platform Module) がサポートされています。Windows オペレーティング・システムがサポートする TPM が Lenovo PC に組み込まれている場合、Client Security Solution は Windows オペレーティング・システムに組み込まれているドライバーを使用します。

TPM はシステムの BIOS によって有効になるため、TPM を使用できるようにするために再起動が必要になる場合があります。 Windows 7 が稼働している場合、システムの起動時に TPM を有効にするかどうかの確認が求められることがあります。

TPM によっていずれかの機能が実施される前に、最初に所有権を初期化する必要があります。各システムは、Client Security Solution オプションを制御する 1 人の Client Security Solution 管理者を持ちます。この管理者は、Windows 管理者権限を持っている必要があります。管理者は XML デプロイメント・スクリプトを使用して初期化することができます。

システムの所有権が構成された後は、このシステムにログインする追加の各 Windows ユーザーに、ユーザーのセキュリティー・キーおよびクレデンシャルを登録し初期化するためのプロンプトが Client Security セットアップ・ウィザードによって自動的に出されます。

TPM のソフトウェア・エミュレーション

Client Security Solution には、限定されたシステム上で TPM を使用せずに実行するオプションが用意されています。この機能は、ハードウェア保護キーを使用する代わりにソフトウェア・ベースのキーを使用する以外は同じです。ソフトウェアは、TPM に効力を与える代わりに、常にソフトウェア・ベースのキーを使用するように強制するスイッチでインストールすることが可能です。このスイッチを使用するかどうかはインストール時の決定で、ソフトウェアのアンインストールおよび再インストールをせずに戻すことはできません。

TPM のソフトウェア・エミュレーションを強制する構文は以下の通りです。

```
InstallFile.exe "/v EMULATIONMODE=1"
```

インストール手順およびコマンド・ライン・パラメーター

Microsoft Windows インストーラーは、コマンド・ライン・パラメーターによって、複数の管理機能を提供します。 Windows インストーラーは、ワークグループによる使用またはカスタマイズのために、アプリケーションまたは製品のネットワークへの管理者用インストールを実行できます。コマンド・ライン・オプションには、パラメーターを指定することが必要です。この場合、オプションとパラメーターの間にスペースは入れません。例:

```
setup.exe /s /v"/qn REBOOT="R""
```

は有効ですが、

```
setup.exe /s /v "/qn REBOOT="R""
```

は無効です。

注: インストールを単独で実行すると (パラメーターを指定せずに setup.exe を実行すると)、デフォルトでは、インストール終了時にユーザーに再起動を促すプロンプトが出されます。プログラムを正しく機能させるには、再起動する必要があります。上記のセクションおよび例のセクションで示すように、サイレント・インストールではコマンド・ライン・パラメーターを使用して再起動を遅らせることができます。

Client Security Solution インストール・パッケージの場合、管理者用インストールによりインストール・ソース・ファイルが指定された場所に解凍されます。

管理者用インストールを実行するには、セットアップ・パッケージをコマンド・ラインから /a パラメーターを使用して実行します。

```
setup.exe /a
```

管理者用インストールは、管理ユーザーにセットアップ・ファイルの解凍先を指定するようプロンプトを出すウィザードを表示します。デフォルトの解凍先は C:¥ です。C:¥ 以外のドライブ (その他のローカル・ドライブ、または割り当てられたネットワーク・ドライブなど) の新しい場所を選択することもできます。新しいフォルダーも、この手順で作成できます。

管理者用インストールをサイレント・インストールで実行する場合、解凍先の場所を指定するために、コマンド・ラインで次のようにパブリック・プロパティ TARGETDIR を設定することができます。

```
setup.exe /s /v"/qn TARGETDIR=F:¥TVTRR"
```

または

```
msiexec.exe /i "Client Security - Password Manager.msi" /qn TARGERDIR=F:¥TVTRR
```

注: 最新バージョンの Windows インストーラーを使用していない場合、Windows インストーラー・エンジンが最新バージョンに更新されるように setup.exe ファイルが構成されます。Windows インストーラー・エンジンの更新の際、管理者用の展開インストールであってもシステムを再起動するようにプロンプトが出されます。この状態の場合に再起動しないようにするには、Windows インストーラーの REBOOT プロパティを使用できます。Windows インストーラーが最新バージョンである場合、setup.exe ファイルは Windows インストーラー・エンジンの更新を試行しません。

管理者用インストールが完了した後、管理者はソース・ファイルをカスタマイズ (たとえば、レジストリーに設定値を追加) することができます。

以下のパラメーターと説明は、InstallShield 開発者のヘルプ文書に記載されています。基本 MSI プロジェクトに適用されないパラメーターは、除かれています。
例: [rescue] mailbox = %y%¥antidote, c:¥antidote

表 2. パラメーター

パラメーター	**説明**
/a : 管理者用インストール	/a スイッチを指定すると、setup.exe で管理者用インストールが実行されます。管理者用インストールは、データ・ファイルをユーザーが指定したディレクトリーにコピー (および解凍) しますが、ショートカットの作成、COM サーバーの登録、アンインストール・ログの作成は行いません。
/x : アンインストール・モード	/x スイッチを指定すると、setup.exe は以前にインストールした製品をアンインストールします。
/s : サイレント・モード	コマンド setup.exe /s を実行すると、基本 MSI インストール・プログラム用の setup.exe 初期設定ウィンドウは表示されず、応答ファイルは読み取られません。基本 MSI プロジェクトでは、サイレント・インストールの場合、応答ファイルは作成も使用もされません。基本 MSI 製品をサイレントで実行するには、コマンド・ライン setup.exe /s /v/qn を実行します。 (基本 MSI のサイレント・インストールのパブリック・プロパティ値を指定する場合は、 setup.exe /s /v″/qn INSTALLDIR=D:¥Destination″ などのコマンドを使用できます。)

表 2. パラメーター (続き)

パラメーター	説明
/v : Msiexec への引数の受け渡し	/v 引数を使用して、 msiexe.exe にコマンド・ライン・スイッチとパブリック・プロパティの値を渡します。
/L : 言語のセットアップ	ユーザーは、/L スイッチと 10 進言語 ID を使用して、複数言語インストール・プログラムで使用する言語を指定します。たとえば、ドイツ語を指定するコマンドは setup.exe /L1031 です。
/w : 待機	基本 MSI プロジェクトで引数 /w を指定すると、setup.exe は、インストールが完了するのを待ってから終了します。バッチ・ファイルで /w オプションを使用すると、 setup.exe のコマンド・ライン引数全体を start /WAIT で開始することができます。正しくフォーマットされたコマンドの使用例は、次のとおりです。 `start /WAIT setup.exe /w`

msiexec.exe の使用

カスタマイズした後に解凍したソースからインストールするには、ユーザーはコマンド・ラインで msiexec.exe を実行し、解凍された *.MSI ファイルの名前を引き渡します。msiexec.exe は、インストール・パッケージを読み取り、製品をターゲット PC にインストールするために使用する Windows インストーラーの実行可能プログラムです。

```
msiexec /i "C:¥WindowsFolder¥Profiles¥UserName¥
Personal¥MySetups¥project name¥product configuration¥release name¥
DiskImages¥Disk1¥product name.msi"
```

注: 上記のコマンドを、円記号の後にスペースを入れずに 1 行として入力します。

次の表では、msiexec.exe で有効なコマンド・ライン・パラメーターと、その使用方法を説明します。

表 3. コマンド・ライン・パラメーター

パラメーター	説明

/I *package*
または
product code
	このフォーマットは製品のインストールに使用します。
	`Othello:msiexec /i "C:¥WindowsFolder¥Profiles¥`
	`UserName¥Personal¥MySetups`
	`¥Othello¥Trial Version¥`
	`Release¥DiskImages¥Disk1¥`
	`Othello Beta.msi"`
	製品コードとは、製品のプロジェクト・ビューの製品コード・プロパティで自動的に生成されるグローバル一意識別子 (GUID) のことです。

表 3. コマンド・ライン・パラメーター (続き)

パラメーター	説明
/a *package*	**/a** オプションにより、管理者権限を持つユーザーは製品をネットワーク上にインストールできます。
/x *package* または *product code*	**/x** オプションは、製品をアンインストールします。
/L [i|w|e|a|r |u|c|m|p|v|+] *log file*	**/L** オプションを使用して作成すると、ログ・ファイルへのパスが指定されます。以下のフラグは、ログ・ファイルに記録する情報を示しています。 • **i** は、状況メッセージをログに記録します • **w** は、致命的でない警告メッセージをログに記録します • **e** は、すべてのエラー・メッセージをログに記録します • **a** は、アクション・シーケンスの開始をログに記録します • **r** は、アクション固有のレコードをログに記録します • **u** は、ユーザー要求をログに記録します • **c** は、初期ユーザー・インターフェース・パラメーターをログに記録します • **m** は、メモリー不足メッセージをログに記録します • **p** は、端末設定をログに記録します • **v** は、冗長出力設定をログに記録します • **+** は、既存ファイルに付加します • ***** は、すべての情報を (冗長出力設定を除いて) ログに記録できるワイルドカード文字です
/q [n|b|r|f]	/q オプションを以下のフラグと併用して、ユーザー・インターフェース・レベルを設定します。 • **q** または qn は、ユーザー・インターフェースを作成しません。 • **qb** は、基本ユーザー・インターフェースを作成します。 下記のユーザー・インターフェース設定により、インストール終了時にモーダル・ダイアログ・ボックスが表示されます。 • **qr** は、縮小ユーザー・インターフェースを表示します。 • **qf** は、完全なユーザー・インターフェースを表示します。 • **qn+** は、ユーザー・インターフェースを表示しません。 • **qb+** は、基本ユーザー・インターフェースを表示します。
/? または /h	いずれかのコマンドにより、Windows インストーラーの著作権情報が表示されます。

表 3. コマンド・ライン・パラメーター (続き)

パラメーター	説明

TRANSFORMS	**TRANSFORMS** コマンド・ライン・パラメーターを使用して、基本パッケージに適用する変換を指定します。
	`msiexec /i "C:¥`*`WindowsFolder`*`¥`
	`Profiles¥`*`UserName`*`¥Personal ¥MySetups¥`
	`Your Project Name¥Trial Version¥`
	`My Release-1 ¥DiskImages¥Disk1¥`
	`ProductName.msi" TRANSFORMS="New Transform 1.mst"`
	複数の変換をセミコロンで分離できます。Windows インストーラー・サービスが誤って解釈しないように、変換の名前にセミコロンを使用しないでください。

Properties	すべてのパブリック・プロパティはコマンド・ラインで設定または変更できます。パブリック・プロパティはプライベート·プロパティと区別され、すべて大文字です。たとえば、*COMPANYNAME* はパブリック・プロパティです。
	コマンド・ラインからプロパティを設定するには、次の構文を使用します。
	`PROPERTY=VALUE`
	COMPANYNAME の値を変更するには、次のように入力します。
	`msiexec /i "C:¥`*`WindowsFolder`*`¥`
	`Profiles¥`*`UserName`*`¥Personal¥`
	`MySetups¥`*`Your Project Name`*`¥`
	`Trial Version¥My Release-1¥`
	`DiskImages¥Disk1¥`*`ProductName.msi`*`"`
	`COMPANYNAME``="InstallShield"`

標準 Windows インストーラーのパブリック・プロパティ

Windows インストーラーには、一連の標準組み込みパブリック・プロパティがあります。これらのプロパティをコマンド・ラインで設定して、インストール時の特定の動作を指定することができます。下表に、コマンド・ラインで使用される最も一般的なパブリック・プロパティについて説明します。

追加情報については、次の Microsoft Web サイトを参照してください。
http://msdn2.microsoft.com/en-us/library/aa367437.aspx

次の表に、一般的に使用される Windows インストーラーのプロパティを示します。

表 4. Windows インストーラーのプロパティ

プロパティ	説明
TARGETDIR	インストール用の宛先のルート・ディレクトリーを指定します。管理者用インストールの場合、このプロパティは、インストール・パッケージのコピー先です。
ARPAUTHORIZEDCDFPREFIX	アプリケーションの更新チャネルの URL。
ARPCOMMENTS	「コントロール パネル」の「プログラムの追加と削除」に「コメント」を提供します。
ARPCONTACT	「コントロール パネル」の「プログラムの追加と削除」に「連絡先」を提供します。
ARPINSTALLLOCATION	アプリケーションの 1 次フォルダーへの完全修飾パス。
ARPNOMODIFY	製品を変更する機能を使用不可にします。
ARPNOREMOVE	製品を削除する機能を使用不可にします。
ARPNOREPAIR	「プログラム」ウィザードの「修復」ボタンを使用不可にします。
ARPPRODUCTICON	インストール・パッケージの基本アイコンを指定します。
ARPREADME	「コントロール パネル」の「プログラムの追加と削除」に README を提供します。
ARPSIZE	アプリケーションの推定サイズ (KB)。
ARPSYSTEMCOMPONENT	「プログラムの追加と削除」のリストにアプリケーションを表示しないようにします。
ARPURLINFOABOUT	アプリケーションのホーム・ページの URL。
ARPURLUPDATEINFO	アプリケーション更新情報の URL。
REBOOT	REBOOT プロパティにより、システムの再起動を促す特定のプロンプトが抑止されます。管理者は通常、一連のインストールを行う際にこのプロパティを使用して、複数の製品を同時にインストールし、最後に一度だけ再起動します。インストール終了時の再起動を使用不可にするには、REBOOT=”R” と設定します。

インストール・ログ・ファイル

Client Security Solution のインストール・ログ・ファイルは cssinstall83xx.log という名前で、setup.exe ファイルでセットアップを起動する (install.exe ファイルをダブルクリックするか、パラメーターなしで実行可能ファイルを実行するか、MSI パッケージを解凍して setup.exe ファイルを実行します) と、%temp% ディレクトリーに作成されます。このファイルには、インストール問題のデバッグに使用できるログ・メッセージが含まれています。このログ・ファイルには、「コントロール パネ

ル」の「**プログラムの追加と削除**」アプレットによって実行されたアクティビティーすべてが含まれます。このログ・ファイルは、MSI パッケージから直接 setup.exe ファイルを実行した場合には作成されません。すべての MSI アクションのログ・ファイルを作成するには、レジストリー内のログ・ポリシーを使用可能にすることができます。これを行うには、次の値を作成します。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥Microsoft¥Windows¥Installer]
"Logging"="voicewarmup"
```

インストールの例

次の表には、setup.exe ファイルを使用したインストールの例が示されています。

表 5. setup.exe ファイルを使用したインストールの例

説明	例
サイレント・インストール (再起動なし)	`setup.exe /s /v"/qn REBOOT="R""`
管理者用インストール	`setup.exe /a`
管理用のサイレント・インストール (Client Security Software の解凍先を指定)。	`setup.exe /a /s /v"/qn TARGETDIR="F:¥CSS83""`
サイレント・アンインストール	`setup.exe /s /x /v/qn`
再起動なしのインストール (Client Security Software の temp サブディレクトリーにインストール・ログを作成)	`setup.exe /v"REBOOT="R" /L*v %temp%¥cssinstall83.log"`
ワークスペースをインストールしないインストール	`setup.exe /vPDA=0`

次の表は、Client Security - Password Manager.msi を使用したインストールの例です。

表 6. Client Security - Password Manager.msi を使用したインストールの例

説明	例
インストール	`msiexec /i "C:¥CSS83¥Client Security Solution - Password Manager.msi"`
サイレント・インストール (再起動なし)	`msiexec /i "C:¥CSS83¥Client Security Solution - Password Manager.msi" /qn REBOOT="R"`
サイレント・アンインストール	`msiexec /x "C:¥CSS83¥Client Security Solution - Password Manager.msi" /qn`

ThinkVantage 指紋認証ソフトウェアのインストール

ThinkVantage 指紋認証ソフトウェア・プログラムの setup.exe ファイルは、以下の方法でインストールできます。

サイレント・インストール

ThinkVantage 指紋認証ソフトウェアをサイレント・インストールするには、CD-ROM ドライブのインストール・ディレクトリーにある setup.exe ファイルを実行します。

このときの構文は次のようになります。

```
Setup.exe PROPERTY=VALUE /q /i
```

ここで、*q* はサイレント・インストール、*i* はインストールを表します。例:

```
setup.exe INSTALLDIR="C:¥Program Files¥ThinkVantage fingerprint software" /q /i
```

このソフトウェアをアンインストールするには、/i の代わりに /x パラメーターを使用します。

```
setup.exe INSTALLDIR="C:¥Program Files¥ThinkVantage fingerprint software" /q /x
```

オプション

ThinkVantage 指紋認証ソフトウェアでは以下のオプションがサポートされています。

表 7. ThinkVantage 指紋認証ソフトウェアでサポートされるオプション

パラメーター	説明
CTRLONCE	コントロール・センターを一度だけ表示します。デフォルト値は 0 です。
CTLCNTR	• 0 = 起動時にコントロール・センターを表示しません。 • 1 = 起動時にコントロール・センターを表示します。 デフォルト値は 1 です。
DEFFUS	• 0 = ユーザーの簡易切り替え (FUS) 設定を使用しません。 • 1 = FUS 設定を使用します。 デフォルト値は 0 です。
DEVICEBIO	ユーザーにより使用されるデバイス・タイプを構成します。 • DEVICEBIO=#3 - デバイス・センサーを使用して最初の登録を保存します。 • DEVICEBIO=#0 - ハードディスク・ドライブを使用して登録を保存します。 • DEVICEBIO=#1 - コンパニオン・チップを使用して登録を保存します。
INSTALLDIR	インストール・ディレクトリーを設定します。
OEM	• 0 = サーバー・パスポートまたはサーバー認証に関するサポートもインストールします。 • 1 = スタンドアロン PC モードのみ (ローカル・パスポート) をインストールします。 デフォルト値は 1 です。

表 7. ThinkVantage 指紋認証ソフトウェアでサポートされるオプション (続き)

パラメーター	説明
PASSPORT	デフォルトのパスポート・タイプを設定します。 • 1 = ローカル・パスポート • 2 = サーバー・パスポート デフォルト値は 1 です。
POSSSO	• 1 = シングル・サインオンを有効にします。 • 0 = シングル・サインオンを無効にします。 デフォルト値は 1 です。
PSLOGON	• 0 = 指紋ログオンを無効にします。 • 1 = 指紋ログオンを有効にします。 デフォルト値は 0 です。
REBOOT	`Really Suppress` に設定すると、インストール中は、プロンプトを含むすべての再起動を行わないようにします。
SECURITY	• 1 = 保護モードでインストールします。 • 0 = 簡易モードでインストールします。
SHORTCUT	• 0 = 起動時にコントロール・センター・ショートカットを表示しません。 • 1 = 起動時のコントロール・センター・ショートカットの表示を有効にします。 デフォルト値は 0 です。
SHORTCUTFOLDER	「**スタート**」メニューのショートカット・フォルダーのデフォルト名を設定します。
非管理者ユーザー特権	
DELETESELF	• 1 = 指紋削除を有効にします。 • 0 = 指紋削除を無効にします。 デフォルト値は 1 です。
ENROLLSELF	• 1 = 指紋登録を有効にします。 • 0 = 指紋登録を無効にします。 デフォルト値は 1 です。
ENROLLTBX	• 1 = パワーオン用の指紋の選択を有効にします。 • 0 = パワーオン用の指紋の選択を無効にします。 デフォルト値は 1 です。

表 7. ThinkVantage 指紋認証ソフトウェアでサポートされるオプション (続き)

パラメーター	説明
IMPORTSELF	• 1 = 管理者以外のユーザーによる指紋のインポート/エクスポートを有効にします。 • 0 = 管理者以外のユーザーによる指紋のインポート/エクスポートを無効にします。 デフォルト値は 1 です。
REVEALPWD	• 1 = Windows パスワードの復元を有効にします。 • 0 = Windows パスワードの復元を無効にします。 デフォルト値は 1 です。
連続再試行に対する保護 (ロックアウト設定)	
LOCKOUT	• 1 = 連続再試行に対する保護を有効にします。 • 0 = 連続再試行に対する保護を無効にします。 デフォルト値は 1 です。
LOCKOUTCOUNT	最大再試行回数。デフォルト値は 5 で、任意の値を使用できます。
LOCKOUTTIME	ミリ秒単位のタイムアウト。デフォルト値は 120 000 で、最大 360 000 までの任意の値を使用できます。
認証タイムアウト (非活動設定)	
GUITMENABLE	• 1 = ミリ秒単位の認証タイムアウトを有効にします。 • 0 = ミリ秒単位の認証タイムアウトを無効にします。 デフォルト値は 1 です。
GUITMTIME	認証タイムアウト期間。デフォルト値は 120 000 で、最大 360 000 までの任意の値を使用できます。
PWDLOGON	• 1 = 管理者以外のユーザーによる指紋認証のみのログオンを有効にします。 • 0 = 管理者以外のユーザーによる指紋認証のみのログオンを無効にします。 デフォルト値は 1 です。
NOPOPPAPCHECK	• 0 = パワーオン・セキュリティー・オプションを表示しません。 • 1 = パワーオン・セキュリティー・オプションを常に表示します。 デフォルト値は 0 です。

表 7. ThinkVantage 指紋認証ソフトウェアでサポートされるオプション (続き)

パラメーター	説明
CSS	• 0 = Client Security Solution はインストールされていないと想定します。 • 1 = Client Security Solution がインストールされていると想定します。 デフォルト値は 0 です。

注: すべてのオプションは任意指定です。

指紋認証ソフトウェアをアンインストールするには、/i ではなく /x パラメーターを使用します。ユーザー・インターフェースからの標準アンインストールの際には、既存のパスポートを削除するかどうか、およびブート・セキュリティー機能を使用不可にするかどうかを選択するためのダイアログが表示されます。サイレント・アンインストール・モードの場合、DELPAS パラメーターを使用できます。既存のパスポートを削除する場合、DELPAS 値を "1" に設定します。これらのオプションを定義しない場合、または他の値にする場合、パスポートは PC 上に残り、ブート・セキュリティーはその後も有効です。ブート・セキュリティーをオンのままにすると、本製品を再インストールしない限りは、ブート・セキュリティー・メモリーで指紋を編集することはできません。例えば、以下の構文を実行するとします。

```
msiexec /i Setup.msi DELPAS="1" /q
```

この場合、製品がアンインストールされ、既存のすべてのパスポートが削除され、ブート・セキュリティーが PC 上に残ります。

Lenovo Fingerprint Software のインストール

Lenovo Fingerprint Software プログラムの setup32.exe ファイルは、以下の手順を使用してインストールできます。

サイレント・インストール

指紋認証ソフトウェアをサイレント・インストールするには、CD-ROM ドライブのインストール・ディレクトリーにある setup32.exe ファイルを実行します。

このときの構文は次のようになります。

```
setup32.exe /s /v"/qn REBOOT ="R""
```

ソフトウェアをアンインストールするには、次の構文を実行します。

```
setup32.exe /x /s /v"/qn REBOOT="R""
```

オプション

Lenovo Fingerprint Software では以下のオプションがサポートされています。

表 8. Lenovo Fingerprint Software でサポートされるオプション

パラメーター	説明
SHORTCUT	「**スタート**」メニューにコントロール・センター・ショートカットを表示します。 • 0 = コントロール・センター・ショートカットを表示しません。 • 1 = コントロール・センター・ショートカットを表示します。 デフォルト値は 0 です。
SWAUTOSTART	• 0 = 起動時に指紋認証ソフトウェアを開始しません。 • 1 = 起動時に指紋認証ソフトウェアを開始します。 デフォルト値は 1 です。
SWFPLOGON	• 0 = 指紋ログオン (GINA またはクレデンシャル・プロバイダー) を使用しません。 • 1 = 指紋ログオン (GINA またはクレデンシャル・プロバイダー) を使用します。 デフォルト値は 0 です。
SWPOPP	• 0 = パワーオン・パスワードの保護を無効にします。 • 1 = パワーオン・パスワードの保護を有効にします。 デフォルト値は 0 です。
SWSSO	• 0 = シングル・サインオン機能を無効にします。 • 1 = シングル・サインオン機能を有効にします。 デフォルト値は 0 です。
SWALLOWENROLL	• 0 = 管理者以外のユーザーによる指紋の登録を無効にします。 • 1 = 管理者以外のユーザーによる指紋の登録を有効にします。 デフォルト値は 1 です。
SWALLOWDELETE	• 0 = 管理者以外のユーザーによる指紋の削除を無効にします。 • 1 = 管理者以外のユーザーによる指紋の削除を有効にします。 デフォルト値は 1 です。

表 8. Lenovo Fingerprint Software でサポートされるオプション (続き)

パラメーター	説明
SWALLOWIMEXPORT	• 0 = 管理者以外のユーザーによる指紋のインポート/エクスポートを無効にします。 • 1 = 管理者以外のユーザーによる指紋のインポート/エクスポートを有効にします。 デフォルト値は 1 です。
SWALLOWSELECT	• 0 = 管理者以外のユーザーが指紋を使用してパワーオン・パスワードを置換することの選択を無効にします。 • 1 = 管理者以外のユーザーが指紋を使用してパワーオン・パスワードを置換することの選択を有効にします。 デフォルト値は 1 です。
SWALLOWPWRECOVERY	• 0 = Windows パスワードの復元を無効にします。 • 1 = Windows パスワードの復元を有効にします。 デフォルト値は 1 です。
SWANTIHAMMER	• 0 = 連続再試行に対する保護を無効にします。 • 1 = 連続再試行に対する保護を有効にします。 デフォルト値は 1 です。
SWANTIHAMMERRETRIES	最大再試行回数を指定します。デフォルト値は 5 です。 **注:** この設定は、SWANTIHAMMER が有効になっているときにのみ、機能します。
SWANTIHAMMERTIMEOUT	タイムアウト期間 (秒単位) を指定します。デフォルト値は 120 です。 **注:** この設定は、SWANTIHAMMER が有効になっているときにのみ、機能します。
SWAUTHTIMEOUT	• 0 = 認証タイムアウトを無効にします。 • 1 = 認証タイムアウトを有効にします。 デフォルト値は 1 です。
SWAUTHTIMEOUTVALUE	認証がタイムアウトになるまでの非アクティブ期間 (秒単位) を指定します。デフォルト値は 120 です。 **注:** この設定は、SWAUTHTIMEOUT が有効になっているときにのみ、機能します。

表 8. Lenovo Fingerprint Software でサポートされるオプション (続き)

パラメーター	説明
SWNONADMIFPLOGONONLY	• 0 = 管理者以外のユーザーによる指紋認証のみのログオンを無効にします。 • 1 = 管理者以外のユーザーによる指紋認証のみのログオンを有効にします。 デフォルト値は 1 です。
SWSHOWPOWERON	• 0 = パワーオン・セキュリティー・オプションを表示しません。 • 1 = パワーオン・セキュリティー・オプションを常に表示します。 デフォルト値は 0 です。
CSS	• 0 = Client Security Solution はインストールされていないと想定します。 • 1 = Client Security Solution がインストールされていると想定します。 デフォルト値は 0 です。

Systems Management Server (SMS)

System Management Server (SMS) のインストールもサポートされています。SMS 管理者コンソールを開きます。新規パッケージを作成して標準的なパッケージ・プロパティを設定します。そのパッケージを開き、「プログラム」項目で「新規プログラム」を選択します。コマンド・ラインに次のように入力します。

```
Setup.exe /m yourmiffilename /q /i
```

サイレント・インストールの場合と同じパラメーターが使用できます。

Setup では、通常はインストール・プロセス終了時に再起動します。インストール中は再起動せず、後で (さらにいくつかのプログラムをインストールしてから) 再起動する場合は、プロパティ・リストに REBOOT=″ReallySuppress″ を追加します。

第 3 章 Client Security Solution での作業

Client Security Solution をインストールする前に、Client Security Solution で選択可能なカスタマイズについて理解する必要があります。この章には、Client Security Solution のカスタマイズに関する情報および TPM (Trusted Platform Module) に関する情報が記載されています。この章では、TPM について Trusted Computing Group (TCG) によって定義された用語を使用します。 TPM について詳しくは、次の Web サイトを参照してください。

http://www.trustedcomputinggroup.org/

TPM の使用

TPM は、 TPM を利用するソフトウェアにセキュリティー関連の機能を提供するために設計されたエンベデッド・セキュリティー・チップです。エンベデッド・セキュリティー・チップは、システムのマザーボードに搭載され、ハードウェア・バスを介して通信します。 TPM を導入しているシステムは、暗号鍵を作成して暗号化することができ、同じ TPM のみが暗号化を解除することができます。このプロセスは、しばしば鍵のラッピング と呼ばれ、鍵の開示を防止するのに役立ちます。 TPM を備えたシステムでは、マスター・ラッピング鍵は、ストレージ・ルート鍵 (SRK) と呼ばれ、 TPM 自体の内部に保存されるので、鍵の秘密 (private) 部分は決して公開されません。エンベデッド・セキュリティー・チップは、他のストレージ・キー、署名鍵、パスワード、およびデータの他の小ユニットも保存できます。 TPM には記憶容量の制限があるので、 SRK はチップ外に記憶するその他の鍵の暗号化に使用されます。 SRK はエンベデッド・セキュリティー・チップに残されることは決してないので、保護ストレージの基本になっています。

エンベデッド・セキュリティー・チップの使用はオプションであり、 Client Security Solution 管理者を必要とします。個人ユーザーでも企業の IT 部門でも、 TPM は初期設定する必要があります。ハードディスク故障からのリカバリーやシステム・ボードの交換など、その後の操作は、Client Security Solution 管理者に限定されます。

注: 認証モードを変更するときにセキュリティー・チップをアンロックしようとする場合、ログアウトしてから、マスター管理者としてログインし直す必要があります。これで、セキュリティー・チップをアンロックすることができます。 2 次ユーザーとしてログオンして、認証モードの変換を続けることもできます。この操作は 2 次ユーザーがログオンすると自動的に行われます。この場合、Client Security Solution によって 2 次ユーザーのパスワードまたはパスフレーズのプロンプトが出されます。 Client Security Solution が変更の処理を完了すると、2 次ユーザーはセキュリティー・チップのアンロック操作に進むことができます。

Windows 7 での TPM の使用

Windows 7 ログオンが有効で、TPM が無効の場合、Windows ログオン機能を無効にしてから、F1 BIOS で TPM を無効にする必要があります。この操作を行うと、「**セキュリティー・チップが非アクティブになりました。ログオン・プロセスを保**

護できません。(Security chip has been deactivated, the logon process cannot be protected)」というセキュリティー・メッセージが表示されなくなります。

さらに、クライアント・システムのオペレーティング・システムをアップグレードする場合、 Client Security の登録に失敗しないためにセキュリティー・チップのクリアが必要です。 F1 BIOS でセキュリティー・チップをクリアするには、システムをコールド起動する必要があります。ウォームリブートの後にこのプロセスを実行しようとすると、セキュリティー・チップをクリアできなくなります。

Client Security Solution の暗号鍵の管理

Client Security Solution については、2 つの主なデプロイメント・アクティビティーである『所有権の取得』と『ユーザー登録』で説明します。 Client Security Solution セットアップ・ウィザードを初めて実行する際に、所有権の取得プロセスとユーザー登録プロセスが、どちらも初期設定時に実行されます。Client Security Solution セットアップ・ウィザードを完了した特定の Windows ユーザー ID は、Client Security Solution 管理者で、アクティブ・ユーザーとして登録されます。システムにログインするその他のユーザーは、すべて Client Security Solution に登録するように自動的に要求されます。

- **所有権の取得**

  単一の Windows 管理者のユーザー ID は、唯一の Client Security Solution 管理者としてシステムに割り当てられます。 Client Security Solution の管理機能は、このユーザー ID により実行される必要があります。 TPM の許可は、このユーザーの Windows パスワードか、Client Security パスフレーズのいずれかです。

  注: 忘れてしまった Client Security Solution 管理者パスワードまたはパスフレーズからリカバリーする唯一の方法は、有効な Windows のアクセス権を使用してこのソフトウェアをアンインストールするか、BIOS 内のセキュリティー・チップをクリアするかのいずれかです。いずれの方法でも、TPM に関連した鍵を介して保護されたデータは、消失します。 Client Security Solution は、忘れてしまったパスワードまたはパスフレーズを自分で復元できるようにするオプション機構も提供します。このため、パスワードまたはパスフレーズは、ユーザー確認のための質問への応答を基にしています。 Client Security Solution 管理者は、この機能を使用するかしないかを決定します。

- **ユーザー登録**

  所有権の取得プロセスが完了し、Client Security Solution 管理者が作成されると、ユーザー・ベース鍵を作成して、現在ログオンしている Windows ユーザーのクレデンシャルを安全に保存することができます。この設計により、複数のユーザーが Client Security Solution に登録し、単一の TPM を利用することができます。ユーザー鍵は、セキュリティー・チップを介して保護されますが、実際にはチップ外のハードディスクに保存されます。この設計では、セキュリティー・チップに構築された実際のメモリーの代わりに、制限のあるストレージ要素としてハードディスク・スペースを作成します。同じセキュア・ハードウェアを利用できるユーザーの数が飛躍的に増大します。

所有権の取得

Client Security Solution のトラステッド・ルートは、システム・ルート・キー (SRK) です。この移動できない非対称鍵は、 TPM のセキュア環境内に生成され、システムに公開されることは決してありません。この鍵を利用する許可は、Windows 管理者アカウントにより TPM_TakeOwnership コマンドの実行中に得られます。Client Security パスフレーズを利用している場合、Client Security Solution 管理者の Client Security パスフレーズは、TPM 許可になり、それ以外の場合は Client Security Solution 管理者の Windows パスワードになります。

システム用に作成された SRK では、その他の鍵ペアは、作成して TPM の外部に保存できますが、ハードウェア・ベースの鍵によってラップまたは保護されます。TPM は SRK を内蔵するハードウェアであり、ハードウェアは損傷することがあるので、システムへの損傷によりデータ・リカバリーが妨げられないようにするためにリカバリー機構が必要です。

システムをリカバリーするために、システム・ベース鍵 (System Base Key) が作成されます。この非対称ストレージ・キーにより、 Client Security Solution 管理者は、システム・ボード交換や別システムへの計画的移行からリカバリーすることができます。システム・ベース鍵を保護しながら、通常の操作またはリカバリー時にアクセスできるようにするために、このキーの 2 つのインスタンスが作成され、異なる 2 つの方法によって保護されます。最初に、システム・ベース鍵は、AES 対称鍵を使用して暗号化されます。この鍵は、Client Security Solution 管理者のパスワードまたは Client Security パスフレーズを知っていれば得ることができます。Client Security Solution リカバリー・キーのこのコピーは、クリアされた TPM またはハードウェア障害により交換されたシステム・ボードからのリカバリー専用です。

Client Security Solution リカバリー・キーの 2 番目のインスタンスは、 SRK によってラップされてキー階層にインポートされます。システム・ベース鍵のこの 2 つのインスタンスにより、 TPM は自身にバインドされた秘密を通常の使用状態で保護することができ、さらに AES 鍵を使用して暗号化されているシステム・ベース鍵を介して、障害のあるシステム・ボードをリカバリーすることができます。AES 鍵は、 Client Security Solution 管理者パスワードまたは Client Security パスフレーズによってアンロックされます。次に、システム・リーフ鍵 (System Leaf Key) が作成されます。このキーは、AES 鍵など、システム・レベルの機密事項を保護するために作成されます。

次の図に、システム・レベルのキー構造を示します。

システム・レベルのキー構造 - 所有権取得

TPM
ストレージ・ルートの秘密鍵
ストレージ・ルートの公開鍵
システム・ベースの秘密鍵
システム・ベースの公開鍵
システム・リーフの秘密鍵
システム・リーフの公開鍵
Auth
1 WAY ハッシュ
CSS 管理者 PW/PP
1 WAY ハッシュ
パスフレーズ (パスワード)
ループが n 回の場合
派生 AES キー経由で暗号化
システム・ベースの秘密鍵
システム・ベースの公開鍵
システム・ベース AES
保護キー
(ハッシュ・アルゴリズムの
出力経由で派生)
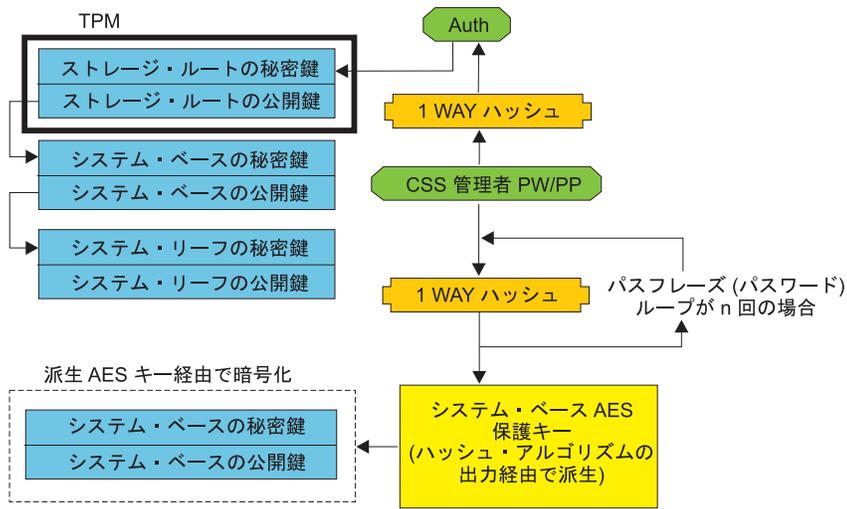
図 1. システム・レベルのキー構造 - 所有権取得

ユーザー登録

各ユーザーのデータを同じ TPM によって保護するために、各ユーザーは独自のユーザー・ベース鍵を作成します。この移動可能な非対称ストレージ・キーは、2 回作成され、各ユーザーの Windows パスワードまたは Client Security パスフレーズから生成された対称 AES 鍵によって保護されます。

次に、ユーザー・ベース鍵の 2 番目のインスタンスは、 TPM にインポートされ、システム SRK によって保護されます。作成されたユーザー・ベース鍵では、ユーザー・リーフ鍵 (User Leaf Key) と呼ばれる第 2 非対称鍵が作成されます。ユーザー・リーフ鍵は、インターネット・ログオン情報の保護に使用される Password Manager AES 鍵、データの保護に使用されるパスワード、およびオペレーティング・システムへのアクセスを防護する Windows パスワード AES 鍵など、個別の秘密事項を保護します。ユーザー・リーフ鍵へのアクセスは、ユーザーの Windows パスワードまたは Client Security Solution パスフレーズによって制御され、ログオン時には自動的にロックが解除されます。

次の図に、ユーザー・レベルのキー構造を示します。

図 2. ユーザー・レベルのキー構造 - ユーザー登録

バックグラウンド登録

Client Security Solution 8.3 は、自動的に開始されるユーザー登録のバックグラウンド登録をサポートします。登録プロセスは、通知を表示せずにバックグラウンドで実行されます。

注: バックグラウンド登録は、自動的に開始されるユーザー登録の場合にのみ、使用できます。「スタート」メニューまたは「**セキュリティー設定のリセット**」から手動で開始されるユーザー登録の場合は、ユーザーがユーザー登録を待機することを示すダイアログが今までどおり表示されます。
ローカル管理者またはドメイン管理者も、次のようにポリシーを編集することで、待機ダイアログを強制的に表示させることができます。

```
CSS_GUI_ALWAYS_SHOW_ENROLLMENT_PROCESSING
```

あるいは、次のようにレジストリー・キーを編集します。

```
HKLM¥software¥policies¥lenovo¥client security solution¥GUI options¥
AlwaysShowEnrollmentProcessing
```

`AlwaysShowEnrollmentProcessing` のデフォルト値は 0 です。上記のレジストリー・キーが 0 に設定された場合は、自動的に開始されるユーザー登録の待機ダイアログは表示されません。このポリシーが 1 に設定された場合は、登録が開始される方法に関係なく、ユーザー登録中に必ず待機ダイアログが表示されます。

ソフトウェア・エミュレーション

TPM を備えていないコンピューターを使用するユーザーの経験レベルを一貫して高めるため、CSS は TPM エミュレーション・モードをサポートしています。

TPM エミュレーション・モードは、トラステッド・ソフトウェア・ベース・ルートです。ユーザーは、TPM によって提供されるのと同じ機能 (デジタル署名、対称鍵暗号化解除、RSA 鍵のインポート、保護、および乱数生成など) を使用可能ですが、トラステッド・ルートはソフトウェア・ベースの鍵であるので、セキュリティーは低下します。

TPM エミュレーション・モードを、TPM のセキュアな代替として使用することはできません。 TPM は、TPM エミュレーション・モードよりセキュアな、次の 2 つの鍵保護方法を提供します。

- TPM によって使用されるすべての鍵が、固有のルート・レベル鍵によって保護されます。固有のルート・レベル鍵は、TPM 内部に作成され、TPM 外部で表示したり使用したりすることはできません。TPM エミュレーション・モードでは、ルート・レベル鍵は、ハードディスク・ドライブに保存されたソフトウェア・ベース鍵です。
- すべての秘密鍵操作は TPM 内部で実行されるので、鍵の秘密鍵の材料が、TPM 外部に露出することはありません。TPM エミュレーション・モードでは、すべての秘密鍵操作がソフトウェア内で実行されるので、秘密鍵の材料は保護されません。

TPM エミュレーション・モードは主に、セキュリティーにはあまり関心がなく、システムのログオン速度に強い関心を持つユーザー向けです。

システム・ボードの交換

システム・ボードを交換するということは、鍵がバインドされていた旧 SRK がもはや無効になり、別の SRK が必要とされていることが推測されます。これは TPM が BIOS によりクリアされても起こります。

Client Security Solution 管理者は、システムのクレデンシャルを新規 SRK にバインドすることを要求されます。システム・ベース鍵は、 Client Security Solution 管理者クレデンシャルから得たシステム・ベース AES 保護鍵により暗号化を解除する必要があります。

Client Security Solution 管理者がドメイン・ユーザー ID であり、そのユーザー ID のパスワードが別のマシン上で変更されていた場合、リカバリーを必要とするシステムにログオンするときに最後に使用されたパスワードが、リカバリーのためにシステム・ベース鍵の暗号化を解除するために既知である必要があります。たとえば、デプロイメント中に、 Client Security Solution 管理者のユーザー ID とパスワードが構成されており、このユーザーのパスワードが別のマシン上で変更されている場合は、デプロイメント中に設定された元のパスワードは、このシステムをリカバリーするための必須権限になります。

以下のステップに従って、システム・ボードの交換を実施してください。

1. Client Security Solution 管理者は、オペレーティング・システムにログオンする。
2. ログオン実行コード (cssplanarswap.exe) は、セキュリティー・チップが使用不可になっていることを認識し、使用可能にするために再起動を要求する (このステップは、BIOS によりセキュリティー・チップを使用可能にすることで回避できます)。
3. システムが再起動され、セキュリティー・チップが使用可能になる。
4. Client Security Solution 管理者がログオンし、次に、新規 Take Ownership プロセスが完了する。
5. システム・ベース鍵は、Client Security Solution 管理者の認証によって得られるシステム基本 AES 保護鍵を使用して暗号化を解除される。システム・ベース鍵は、新規 SRK にインポートされて、システム・リーフ鍵とそれによって保護されているすべてのクレデンシャルを再設定します。
6. これで、システムはリカバリーされます。

注: システム・ボードの交換は、エミュレーション・モードの使用時は必要ありません。

次の図に、マザーボード・スワップ (所有権取得) の構造を示します。
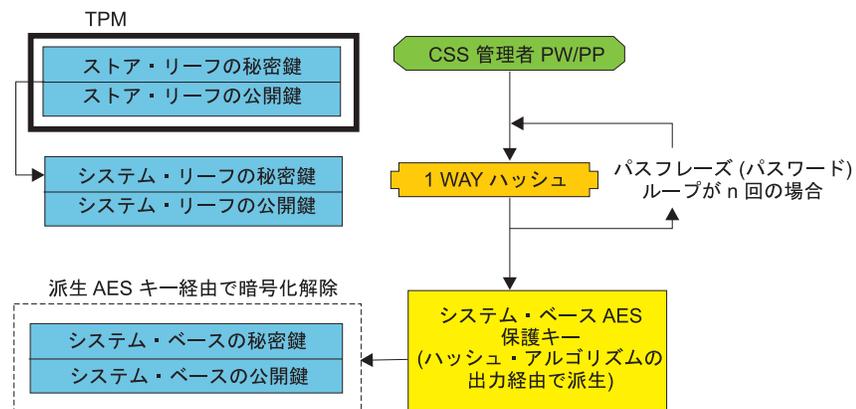
図 3. システム・ボードの交換 - 所有権取得

各ユーザーがシステムにログオンする度に、ユーザー・ベース鍵がユーザー認証から得られるユーザー・ベース AES 保護鍵により自動的に暗号化を解除され、Client Security Solution 管理者により作成された新規 SRK にインポートされます。次の図に、マザーボード・スワップ (ユーザー登録) の構造を示します。

セキュリティー・チップのクリア後、またはマザーボードの交換後に 2 次ユーザーをログインさせるには、マスター管理者としてログインする必要があります。マスター管理者には鍵を復元するためのプロンプトが出されます。鍵の復元が完了したら、Policy Manager を使用して Client Security の Windows ログオンを無効にします。残りのユーザーはそれぞれの鍵を復元できます。すべての 2 次ユーザーがそれ

ぞれの鍵を復元したら、マスター管理者は Client Security Solution の Windows ログオン機能を有効にすることができます。

次の図に、マザーボード・スワップ (ユーザー登録) の構造を示します。
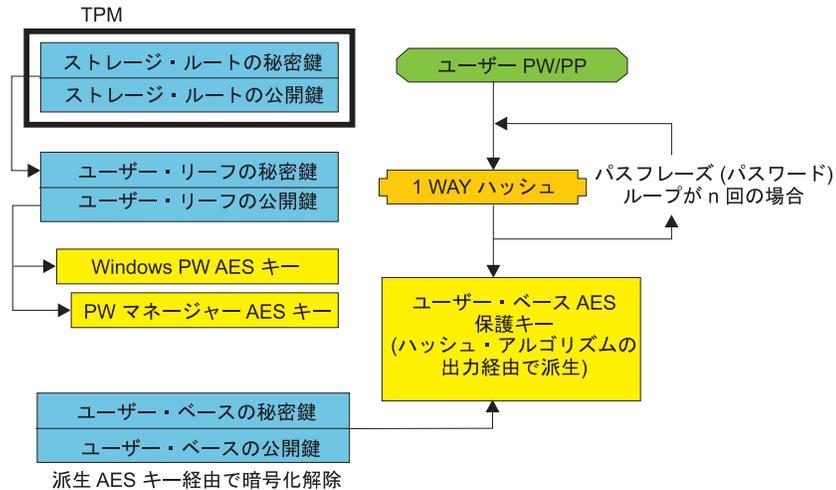
図 4. マザーボード・スワップ - ユーザー登録

EFS 保護ユーティリティー

Client Security Solution は、ファイルおよびフォルダーを暗号化するために Encrypting File System (EFS) が使用する暗号化証明書を、TPM に基づいて保護できるようにするコマンド・ライン・ユーティリティーを提供します。このユーティリティーは、サード・パーティー証明書 (認証局が生成する証明書) の転送をサポートし、さらに自己署名証明書の生成もサポートします。

Client Security Solution による EFS 証明書の保護とは、EFS 証明書に関連する秘密鍵が TPM によって保護されることを意味します。この証明書へのアクセスは、ユーザーが Client Security Solution で認証された後に認可されます。

TPM が有効でない場合、EFS 証明書は Client Security Solution が提供する TPM エミュレーターを使用して保護されます。EFS 証明書が Client Security Solution によって保護されるようにするには、Client Security Solution への登録が必要です。

注意:
Client Security Solution と Encrypting File System (EFS) を使用してファイルおよびフォルダーを暗号化した場合、Client Security Solution または TPM が使用できない場合には暗号化されたファイルにアクセスできません。

TPM が反応しなくなった場合、Client Security Solution はマザーボードを交換した後に暗号化されたデータへ再びアクセスできるようになります。

EFS コマンド・ライン・ユーティリティーの使用

次の表に、EFS でサポートされるコマンド・ライン・パラメーターを示します。

表 9. EFS でサポートされるコマンド・ライン・パラメーター

パラメーター	説明
/generate:<size>	自己署名証明書を生成し、その証明書を EFS に関連付けます。 <size> を指定すると、生成される鍵は指定されたビット・サイズのものになります。有効な値は、512、1024、および 2048 です。値を指定しない場合、または無効値を指定すると、デフォルトで 1024 ビットの鍵が生成されます。
/sn:xxxxxx	転送して EFS と関連付ける既存の証明書のシリアル番号を指定します。
/cn:yyyyyy	転送して EFS と関連付ける既存の証明書の名前 (「発行先」) を指定します。
/firstavail	最初に使用可能な既存の EFS 証明書を転送して EFS と関連付けます。
/silent	出力を表示しません。プログラム終了時に値によって提供される戻りコード。
/? または /h または /help	ヘルプ情報を表示します。

サイレント・モードで実行されていない場合、このユーティリティーは以下のいずれかのエラーを戻します。

```
0 - "Command completed successfully"
1 - "This utility requires Windows XP"
2 - "This utility requires Client Security Solution version 8.0"
3 - "The current user is not enrolled with Client Security Solution"
4 - "The specified certificate could not be found"
5 - "Unable to generate a self-signed certificate"
6 - "No EFS certificates were found"
7 - "Unable to associate the certificate with EFS"
```

サイレント・モードで実行されている場合、プログラムの出力は、上記に示すエラー番号に対応するエラー・レベルになります。

XML スキーマの使用

XML スクリプト記述の目的は、IT 管理者が Client Security Solution のデプロイおよび構成に使用できるカスタム・スクリプトを作成できるようにすることです。スクリプトは xml_crypt_tool 実行可能モジュールによって保護できます (AES 暗号化などのパスワードを使用)。いったん作成されると、仮想マシン (vmserver.exe) は、入力としてスクリプトを受け入れます。仮想マシンは、Client Security Solution セットアップ・ウィザードと同一のファンクションを呼び出して、ソフトウェアを構成します。

すべてのスクリプトは、XML エンコード・タイプ、XML スキーマ、および実行する 1 つ以上の機能を指定する 1 つのタグより構成されています。スキーマは、XML ファイルを検証し、必須パラメーターがそろっていることを確認するために使用されます。スキーマの使用は、現在、推奨されていません。各ファンクション

は、ファンクション・タグで囲まれています。各ファンクションには ORDER が含まれています。これは、コマンドが仮想マシン (vmserver.exe) によって実行される順番を指定します。各ファンクションには、バージョン番号も含まれます。現在、すべてのファンクションはバージョン 1.0 です。以下のスクリプト例には、それぞれ 1 つのファンクションのみが含まれています。しかし、実際のスクリプトには複数のファンクションが含まれる可能性が高くなります。 Client Security Solution セットアップ・ウィザードを使用すれば、このようなスクリプトを作成できます。セットアップ・ウィザードによるスクリプト作成の追加情報については、 47 ページの『Client Security Solution セットアップ・ウィザード』を参照してください。

注: ドメイン名を必要とするファンクションのいずれかに、パラメーター <DOMAIN_NAME_PARAMETER> が残されている場合は、システムのデフォルトの PC 名が使用されます。

例

以下のコマンドは、XML スキーマの例です。

ENABLE_TPM_FUNCTION

このコマンドは、TPM を使用可能にし、引数 SYSTEM_PAP を使用します。システムに既に BIOS 管理者またはスーパーバイザー・パスワードが設定されている場合は、この引数を指定する必要があります。それ以外の場合、このコマンドはオプションです。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

DISABLE_TPM_FUNCTION

このコマンドは引数 SYSTEM_PAP を使用します。システムに既に BIOS 管理者またはスーパーバイザー・パスワードが設定されている場合は、この引数を指定する必要があります。それ以外の場合、このコマンドはオプションです。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>DISABLE_TPM_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
          <SYSTEM_PAP>password</SYSTEM_PAP>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

ENABLE_PWMGR_FUNCTION

このコマンドは、すべての Client Security Solution ユーザーに対して Password Manager を使用可能にします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
  <CSSFile xmlns="www.lenovo.com/security/CSS">
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_PWMGR_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_CSS_GINA_FUNCTION

Windows XP、Windows Vista、および Windows 7 の場合、次のコマンドで Client Security Solution ログオンが可能になります。

```
- <tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_CSS_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_FUNCTION

注:

1. このコマンドは ThinkVantage 指紋認証ソフトウェア専用です。
2. このコマンドは、エミュレーション・モードではサポートされていません。

次のコマンドでは、ThinkVantage 指紋認証による Windows ログオンが有効になり、Client Security Solution による Windows ログオンが無効になります。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
         <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_UPEK_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_UPEK_GINA_WITH_FUS_FUNCTION

注:

1. このコマンドは ThinkVantage 指紋認証ソフトウェア専用です。
2. このコマンドは、エミュレーション・モードではサポートされていません。

次のコマンドでは、ユーザーの簡易切り替えがサポートされるログオンが有効になり、Client Security Solution による Windows ログオンが無効になります。PC がドメイン環境にある場合には、ユーザーの簡易切り替えは無効です。これは、Microsoft の設計です。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
     <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_UPEK_GINA_WIH_FUS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_AUTHENTEC_GINA_FUNCTION

注:

1. このコマンドは Lenovo Fingerprint Software 専用です。
2. このコマンドは、エミュレーション・モードではサポートされていません。

次のコマンドでは、Lenovo Fingerprint による Windows ログオンが有効になり、Client Security Solution による Windows ログオンが無効になります。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment >
         <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_AUTHENTEC_GINA_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_AUTHENTEC_GINA_WITH_FUS_FUNCTION

注:

1. このコマンドは Lenovo Fingerprint Software 専用です。
2. このコマンドは、エミュレーション・モードではサポートされていません。

次のコマンドでは、ユーザーの簡易切り替えがサポートされるログオンが有効になり、Client Security Solution による Windows ログオンが無効になります。PC がドメイン環境にある場合には、ユーザーの簡易切り替えは無効です。これは、Microsoft の設計です。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
     <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_AUTHENTEC_GINA_WIH_FUS_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

ENABLE_NONE_GINA_FUNCTION

ThinkVantage 指紋認証ソフトウェア、Client Security Solution、または Access Connections などの ThinkVantage Technology 関連コンポーネントのいずれかの GINA または CP (クレデンシャル・プロバイダー) が使用可能な場合、このコマンドは ThinkVantage 指紋認証ソフトウェアのログオンと Client Security Solution のログオンの両方を使用不可にします。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENABLE_CSS_NONE_FUNCTION</COMMAND>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

SET_PP_FLAG_FUNCTION

このコマンドは、Client Security パスフレーズを使用するか、Windows パスワードを使用するかを決めるために、Client Security Solution が読み取るフラグを書き込みます。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
         <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>SET_PP_FLAG_FUNCTION</COMMAND>
         <PP_FLAG_SETTING_PARAMETER>USE_CSS_PP</PP_FLAG_SETTING_PARAMETER>
         <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

SET_ADMIN_USER_FUNCTION

このコマンドは、管理者を決めるために Client Security Solution が読み取るフラグを書き込みます。パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  管理者のユーザー名。

- **DOMAIN_NAME_PARAMETER**

  管理者のドメイン名。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>SET_ADMIN_USER_FUNCTION</COMMAND>
```

```
        <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
        <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
       <VERSION>1.0</VERSION>
        <SYSTEM_PAP>PASSWORD</SYSTEM_PAP>
       </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

INITIALIZE_SYSTEM_FUNCTION

このコマンドは、Client Security Solution システム機能を初期設定します。システム全体の鍵は、このファンクション呼び出しにより生成されます。次のパラメーター・リストで、各ファンクションについて説明します。

- **NEW_OWNER_AUTH_DATA_PARAMETER**

  このパラメーターは、システムの新規所有者パスワードを設定するために使用されます。新規所有者パスワードの場合、このパラメーターの値は現行所有者パスワードにより制御されます。現行所有者パスワードが設定されていない場合、このパラメーターの値が渡されて新規所有者パスワードになります。現行所有者パスワードが既に設定され、管理者が同じ現行の所有者パスワードを使用する場合は、このパラメーターの値が渡されます。管理者が新規所有者パスワードを使用する場合、新規所有者パスワードがこのパラメーターに渡されます。

- **CURRENT_OWNER_AUTH_DATA_PARAMETER**

  このパラメーターは、システムの現行所有者パスワードです。既にシステムに既存の所有者パスワードがある場合は、このパラメーターは前のパスワードを渡す必要があります。新規所有者パスワードが要求される場合、現行所有者パスワードがこのパラメーターに渡されます。パスワード変更が構成されていない場合は、値 NO_CURRENT_OWNER_AUTH が渡されます。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
       <FUNCTION>
        <ORDER>0001</ORDER>
        <COMMAND>INITIALIZE_SYSTEM_FUNCTION</COMMAND>
        <NEW_OWNER_AUTH_DATA_PARAMETER>pass1word</NEW_OWNER_AUTH_DATA_
            PARAMETER>
        <CURRENT_OWNER_AUTH_DATA_PARAMETER>No_CURRENT_OWNER_AUTH</CURRENT
            _OWNER_AUTH_DATA_PARAMETER>
       <VERSION>1.0</VERSION>
       </FUNCTION>
</CSSFile>
```

CHANGE_TPM_OWNER_AUTH_FUNCTION

このコマンドは、Client Security Solution 管理者権限を変更し、それに応じてシステム鍵を更新します。システム全体の鍵は、このファンクション呼び出しにより再生成されます。パラメーターは次のとおりです。

- NEW_OWNER_AUTH_DATA_PARAMETER

  TPM の新規所有者パスワード

- CURRENT_OWNER_AUTH_DATA_PARAMETER

  TPM の現行所有者パスワード

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>CHANGE_TPM_OWNER_AUTH_FUNCTION</COMMAND>
          <NEW_OWNER_AUTH_DATA_PARAMETER>newPassWord</NEW_OWNER_AUTH_DATA_
              PARAMETER>
          <CURRENT_OWNER_AUTH_DATA_PARAMETER>oldPassWord</CURRENT_OWNER_AUTH
              _DATA_PARAMETER>
         <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

注: このコマンドは、エミュレーション・モードではサポートされていません。

ENROLL_USER_FUNCTION

このコマンドは、Client Security Solution を使用する特定のユーザーを登録します。このファンクションは、ユーザー固有のセキュリティー・キーのすべてを所定のユーザーに作成します。 パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  登録するユーザーのユーザー名

- **DOMAIN_NAME_PARAMETER**

  登録するユーザーのドメイン名

- **USER_AUTH_DATA_PARAMETER**

  ユーザーのセキュリティー・キーを作成するための TPM パスフレーズまたは Windows パスワード

- **WIN_PW_PARAMETER**

  Windows パスワード

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>ENROLL_USER_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_AUTH_DATA_PARAMETER>myCssUserPassPhrase</USER_AUTH_DATA_PARAMETER>

          <WIN_PW_PARAMETER>myWindowsPassword</WIN_PW_PARAMETER>
         <VERSION>1.0</VERSION>
          </FUNCTION>
</CSSFile>
```

USER_PW_RECOVERY_FUNCTION

このコマンドは、特定ユーザーのパスワード・リカバリーをセットアップします。パラメーターは次のとおりです。

- **USER_NAME_PARAMETER**

  登録するユーザーのユーザー名
- **DOMAIN_NAME_PARAMETER**

  登録するユーザーのドメイン名
- **USER_PW_REC_QUESTION_COUNT**

  ユーザーが応答しなければならない質問の数
- **USER_PW_REC_ANSWER_DATA_PARAMETER**

  特定の質問に対する、保存されている応答。このパラメーターの実名には、応答される質問に対応する番号が連結しています。
- **USER_PW_REC_STORED_PASSWORD_PARAMETER**

  質問のすべてが正確に応答されると、ユーザーに示される保存されたパスワード。

```
<tvt_deployment xmlns ="http://www.lenovo.com"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance " xsi:schemaLocation="
http://www.lenovo.com cssDeploy.xsd">
  < registry_settings />
  < /tvt_deployment
          <FUNCTION>
          <ORDER>0001</ORDER>
          <COMMAND>USER_PW_RECOVERY_FUNCTION</COMMAND>
          <USER_NAME_PARAMETER>sabedi</USER_NAME_PARAMETER>
          <DOMAIN_NAME_PARAMETER>IBM-2AA92582C79<DOMAIN_NAME_PARAMETER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test1</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test2</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_ANSWER_DATA_PARAMETER>Test3</USER_PW_REC_ANSWER_DATA_PARA
              METER>
          <USER_PW_REC_QUESTION_COUNT>3</USER_PW_REC_QUESTION_COUNT>
          <USER_PW_REC_QUESTION_LIST>20000,20001,20002</USER_PW_REC_QUESTION_LIST>
         </USER_PW_REC_STORED_PASSWORD_PARAMETER>Pass1word</USER_PW_REC_STORED_PASS
              WORD_PARAMETER>
          <VERSION>1.0</VERSION>
         </FUNCTION>
</CSSFile>
```

GENERATE_MULTI_FACTOR_DEVICE_FUNCTION

このコマンドは、認証に使用される Client Security Solution の多層デバイスを生成します。パラメーターは次のとおりです。

- USER_NAME_PARAMETER - 管理者のユーザー名。
- DOMAIN_NAME_PARAMETER - 管理者のドメイン名。
- MULTI_FACTOR_DEVICE_USER_AUTH - ユーザーのセキュリティー・キーを作成するための Client Security パスフレーズまたは Windows パスワード。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
```

```
<ORDER>0001</ORDER>
<COMMAND>GENERATE_MULTI_FACTOR_DEVICE_FUNCTION</COMMAND>
<USER_NAME_PARAMETER>myUserName</USER_NAME_PARAMETER>
<DOMAIN_NAME_PARAMETER>domainName</DOMAIN_NAME_PARAMETER>
<MULTI_FACTOR_DEVICE_USER_AUTH>myCssUserPassPhrase</MULTI_FACTOR_DEVICE_USER_AUTH>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

SETUP_PDA_FUNCTION

このコマンドは、Client Security Solution と使用するために Rescue and Recovery ワークスペースをセットアップします。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
<ORDER>0001</ORDER>
<COMMAND>SETUP_PDA_FUNCTION</COMMAND>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

SET_USER_AUTH_FUNCTION

このコマンドは、Client Security Solution のユーザー認証を設定します。

```
<?xml version="1.0" encoding="UTF-8" standalone="no" ?>
<CSSFile=xmlns="www.ibm.com/security/CSS">
<FUNCTION>
<ORDER>0001</ORDER>
<COMMAND>SET_USER_AUTH_FUNCTION</COMMAND>
<VERSION>1.0</VERSION>
</FUNCTION>
</CSSFile>
```

スマート・カードの使用

スマート・カードによってセキュリティー・レベルが強化されます。Client Security Solution 8.3 はユーザー認証にスマート・カードを使用する企業を支援するように設計されており、スマート・カードのサポートと機能を備えています。スマート・カードは、Client Security Solution が Windows ログオンや Password Manager などのユーザー認証を必要とする場合に、システムへのログオンに使用できます。

スマート・カード・パッケージのインストール

スマート・カード・ミドルウェアは、Lenovo Web サイトで入手できます。または、スマート・カード製造元から、最新リリースのスマート・カード・ミドルウェアを取得することもできます。

要件

次のリストに、スマート・カード機能を持つ Client Security Solution の要件を示します。

- スマート・カード・リーダーは内部に取り付けるか、USB (ユニバーサル・シリアル・バス) ポートを介して接続する必要があります。
- スマート・カードを Client Security Solution で使用するには、登録が必要です。スマート・カードの登録場所には、Client Security Solution からアクセスできます。

- ユーザーごとに 1 つのスマート・カードのみが登録可能です。
- デジタル署名用のスマート・カードには、少なくとも 1 つの証明書がなければなりません。カード上で複数の有効な証明書が検出されると、いずれか 1 つの証明書を選択するようにプロンプトで指示されます。
- スマート・カードの構成には必ず PIN を使用してください。

スマート・カードの働き

スマート・カードはクレジット・カードのサイズで、内部にチップが埋め込まれています。スマート・カードをカード・リーダーに挿入すると、スマート・カードに埋め込まれたチップに格納されているデータが読み取られます。

スマート・カードの登録

スマート・カード・リーダーが検出されると、スマート・カードを Client Security Solution に登録することができます。スマート・カード・リーダーが検出されない場合、このオプションは無効になります。スマート・カードの登録および登録解除を行っても、Client Security Solution クレデンシャルは失われません。

PIN

プロンプトが出されたら、スマート・カードの PIN を入力する必要があります。スマート・カードを挿入すると、その PIN が検証されます。 PIN の検証後、最初に登録された証明書がユーザー認証に使用されます。 Client Security Solution では、スマート・カード PIN の入力の最大再試行回数は適用されません。入力した PIN で失敗した場合、PIN の再入力を求めるプロンプトが出されます。

Policy Manager のサポート

Policy Manager では、認証装置としてスマート・カードを使用することを選択できます。パスワードまたはパスフレーズの使用を選択すると、Policy Manager でポリシーを設定することによりスマート・カードをオーバーライドすることができます。

すべてのユーザーについてスマート・カードを登録解除する場合、Client Security Solution の Policy Manager でスマート・カード・ポリシー・オプションをオフにすることをお勧めします。

RSA SecurID トークンの使用

データ暗号化の暗号化アルゴリズム方式を利用すると、Client Security Solution に加えて RSA SecurID トークンを使用することにより、お客様の企業に多層セキュリティーが提供されます。 RSA SecurID トークンを使用して、ユーザーはユーザー ID または PIN、およびトークン・デバイスを使用してネットワークやソフトウェアで認証され、ログインすることができます。トークン・デバイスは、60 秒ごとに変わる数字のストリングを表示します。この認証方式では、再使用可能なパスワードと比較して格段に信頼性の高いユーザー認証が可能になります。

RSA SecurID ソフトウェア・トークンのインストール

RSA SecurID ソフトウェアをインストールするには、次のステップを実行します。

1. 次の Web サイトに進む。

   http://www.rsasecurity.com/node.asp?id=1156
2. 登録プロセスを完了します。
3. RSA SecurID ソフトウェアをダウンロードおよびインストールします。

要件

1. RSA ソフトウェアが Client Security Solution と関連付けられた後に正しく動作するには、各 Windows ユーザーが Client Security Solution に登録する必要があります。
2. Windows ユーザーが Client Security Solution に登録していないと、そのユーザーを認証しようとして、RSA ソフトウェアはエンドレス・ループに陥ります。ユーザーを Client Security Solution に登録するとこの問題は解決します。

スマート・カード・アクセス・オプションの設定

スマート・カード・アクセス・オプションを設定するには、次のステップを実行します。

1. RSA SecurID メインメニューから、「**Tools (ツール)**」、「**Smart Card Access Options (スマート・カード・アクセス・オプション)**」の順にクリックします。
2. 「Smart Card Communication (スマート・カード通信)」パネルから、「**Access the Smart Card through a PKCS #11 module (PKCS #11 モジュールを使用してスマート・カードにアクセス)**」のラジオ・ボタンを選択します。
3. 「**Browse (参照)**」ボタンをクリックして、次のパスまでナビゲートします。

   ```
   C:¥Program Files¥LENOVO¥Client Security Solution¥csspkcs11.dll
   ```
4. **csspkcs11.dll** ファイルをクリックし、「**Select (選択)**」をクリックします。
5. 「**OK**」をクリックします。

RSA SecurID ソフトウェア・トークンの手動インストール

RSA SecurID ソフトウェア・トークンによる Client Security Solution 保護を利用するには、次のステップを実行します。

1. RSA SecurID ソフトウェア・トークンのメインメニューから、「**File (ファイル)**」、「**Import Tokens (トークンのインポート)**」の順にクリックします。
2. SDTID ファイルの場所までナビゲートし、「**Open (開く)**」をクリックします。
3. 「**Select Token(s) to Install (インストールするトークンの選択)**」パネルから、インストールしたいソフトウェア・トークンのシリアル番号を強調表示します。
4. 「**Transfer Selected Tokens Smart Card (選択したトークンのスマート・カードを転送)**」をクリックします。

   注: トークンに配布パスワードがある場合、プロンプトが出されたらそのパスワードを入力します。
5. 「**OK**」をクリックします。

Active Directory のサポート

次のパスは Client Security Solution の PKCS #11 モジュールがあるディレクトリー・パスを示します。

```
C:¥Program Files¥Lenovo¥Client Security Solution¥csspkcs11.dll
```

Client Security Solution の PKCS #11 モジュールを利用するには、Active Directory に以下のポリシーを設定する必要があります。

1. PKCS #11 署名
2. PKCS #11 暗号化解除

次の表に、PKCS# 11 のポリシーの変更可能フィールドと説明を示します。

表 10. ThinkVantage¥Client Security Solution¥Authentication Policies¥PKCS# 11 Signature¥Custom Mode

フィールド	CSS.ADM
変更可能フィールド	必須
フィールドの説明	パスワード、パスフレーズ、またはスマート・カードが必要であるかどうかを制御します。
可能な値	• Enabled (有効) – Every time (毎回) – Once per logon (ログオンごと) • Disabled (無効) • Not configured (構成されない)

指紋センサー認証の設定とポリシー

強制的な指紋バイパス・オプション

指紋バイパス・オプションを使用すると、ユーザーは、指紋認証をバイパスでき、Windows パスワードを使用してログオンできます。ユーザーは、新しい登録を追加するときに、Password Manager のユーザー・インターフェースでこのオプションを選択または選択解除できます。

ただし、デフォルトでは、このオプションが選択されていない場合でも、指紋バイパスは有効になります。これは、指紋センサーが機能しなくても、ユーザーが Windows にログオンできるようにするためです。強制的な指紋バイパス・オプションを無効にするには、次のレジストリー・キーを編集します。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Lenovo¥Client Security Solution¥CSS Configuration]
"GinaDenyLogonDeviceNonEnrolled"=dword:00000001
```

レジストリー・キーが上記のように設定されると、ユーザーは、指紋センサーが機能しないときにも指紋認証をバイパスできません。

指紋の読み取り結果

指紋認証中は、下記のポリシーによって、指紋の読み取り結果の表示が制御されます。

```
HKLM¥Lenovo¥TVT Common¥Client Security Solution¥FPSwipeResult
```

- FPSwipeResult=0: すべてのメッセージを表示します。
- FPSwipeResult=1: 失敗のメッセージのみを表示します (デフォルト値)。
- FPSwipeResult=2: メッセージを表示しません。

コマンド・ライン・ツール

企業の IT 管理者はコマンドライン・インターフェースを使用して、ローカルまたはリモートから ThinkVantage テクノロジーの機能を実装することもできます。設定情報は、リモートのテキスト・ファイル設定を介して保守することができます。

Client Security Solution には次のコマンド・ライン・ツールがあります。

- 『Security Advisor』
- 47 ページの『Client Security Solution セットアップ・ウィザード』
- 48 ページの『デプロイメント・ファイルの暗号化または暗号化解除ツール』
- 48 ページの『デプロイメント・ファイル処理ツール』
- 49 ページの『TPMENABLE.EXE』
- 49 ページの『証明書転送ツール』
- 50 ページの『TPM 有効化ツール』

Security Advisor

Security Advisor 機能を使用するには、Client Security Solution を起動してから、「**拡張**」メニューをクリックして、Client Security Solution ワークスペースの「**Security Advisor**」ボタンをクリックします。システムは wst.exe ファイルを実行します。デフォルトのインストール済み環境では、このファイルは C:¥Program Files¥Lenovo¥Common Files¥WST¥ ディレクトリーにあります。

パラメーターは次のとおりです。

表 11. パラメーター

パラメーター	**説明**
HardwarePasswords	ハードウェア・パスワードの値を設定します。1 はこのセクションを表示し、0 は隠します。デフォルト値は 1 です。
PowerOnPassword	パワーオン・パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
HardDrivePassword	ハードディスクのパスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
AdministratorPassword	管理者パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。

表 11. パラメーター (続き)

パラメーター	説明
WindowsUsersPasswords	Windows ユーザー・パスワードの値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
Password	ユーザー・パスワードを使用可能にする値か、設定にフラグを立てる値を設定します。
PasswordAge	このマシン上での、Windows パスワードの使用日数の値を設定するか、設定にフラグを立てる値を設定します。
PasswordNeverExpires	Windows のパスワードが期限切れにならない値を設定するか、設定にフラグを立てる値を設定します。
WindowsPasswordPolicy	Windows パスワード・ポリシーの値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
MinimumPasswordLength	このマシン上でのパスワードの長さの値を設定するか、設定にフラグを立てる値を設定します。
MaximumPasswordAge	このマシン上でのパスワードの使用日数の値を設定するか、設定にフラグを立てる値を設定します。
ScreenSaver	スクリーン・セーバーの値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
ScreenSaverPasswordSet	スクリーン・セーバーにパスワードを要求する値を設定するか、設定にフラグを立てる値を設定します。
ScreenSaverTimeout	このマシン上でのスクリーン・セーバーのタイムアウトの値を設定するか、設定にフラグを立てる値を設定します。
FileSharing	ファイル共有の値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
AuthorizedAccessOnly	ファイル共有のための許可されたアクセスを設定する値を設定するか、設定にフラグを立てる値を設定します。
ClientSecurity	Client Security の値を設定します。1 はこのセクションを表示し、0 は隠します。このパラメーターが表示されていない場合は、デフォルトで表示されます。
EmbeddedSecurityChip	セキュリティー・チップを使用可能にする値を設定するか、設定にフラグを立てる値を設定します。

表 11. パラメーター (続き)

パラメーター	説明
ClientSecuritySolution	このマシン上で使用する Client Security Solution のバージョンの値を設定するか、設定にフラグを立てる値を設定します。

Client Security Solution セットアップ・ウィザード

Client Security Solution セットアップ・ウィザードは、XML ファイルを介してデプロイメント・スクリプトを生成する際に使用します。次のコマンドを実行すると、ウィザードのさまざまな機能が表示されます。

```
"C:¥Program Files¥Lenovo¥Client Security Solution¥css_wizard.exe" /?
```

次の表に、Client Security Solution セットアップ・ウィザードのコマンドを示します。

表 12. Client Security Solution セットアップ・ウィザードのコマンド

パラメーター	結果
/h または /?	ヘルプ・メッセージ・ボックスを表示します
/name:*FILENAME*	生成されたデプロイメント・ファイルの完全修飾パスおよびファイル名の前に付けます。このファイルには拡張子 .xml が付きます。
/encrypt	AES 暗号化を使用してスクリプト・ファイルを暗号化します。暗号化される場合、そのファイル名には .enc が付加されます。 /pass コマンドを使用しない場合は、静的パスフレーズを使用して、ファイルを隠します。
/pass:	暗号化されたデプロイメント・ファイルを保護するために、パスフレーズの前に付けます。
/novalidate	ウィザードのパスワードとパスフレーズのチェック機能を使用不可にして、すでに構成済みのマシン上でスクリプト・ファイルを作成できるようにします。たとえば、現行マシンの管理者パスワードは、社内で要求される管理者パスワードではないことがあります。/novalidate コマンドを使用するとユーザーは xml ファイル作成中に css_wizard GUI に別の管理者パスワードを入力できます。

例:

```
css_wizard.exe /encrypt /pass:my secret /name:C:¥DeployScript /novalidate
```

デプロイメント・ファイルの暗号化または暗号化解除ツール

このツールは Client Security XML デプロイメント・ファイルの暗号化または暗号化解除に使用します。次のコマンドを実行すると、ツールのさまざまな機能が表示されます。

```
"C:¥Program Files¥Lenovo¥Client Security Solution¥xml_crypt_tool.exe" /?
```

パラメーターを次の表に示します。

表 13. Client Security XML デプロイメント・ファイルを暗号化または暗号化解除するためのパラメーター

パラメーター	結果
/h または /?	ヘルプ・メッセージを表示します。
FILENAME	.xml または .enc の拡張子を持つパス名およびファイル名を表示します。
/encrypt または /decrypt	XML ファイルには /encrypt を、ENC ファイルには /decrypt を選択します。
PASSPHRASE	ファイルを保護するためにパスフレーズを使用する場合に必要なオプション・パラメーターを表示します。

例:

```
xml_crypt_tool.exe "C:¥DeployScript.xml" /encrypt "my secret"
```

および

```
xml_crypt_tool.exe "C:¥DeployScript.xml.enc" /decrypt "my secret"
```

デプロイメント・ファイル処理ツール

ツール vmserver.exe は Client Security Solution XML デプロイメント・スクリプトを処理します。次のコマンドを実行すると、ウィザードのさまざまな機能が表示されます。

```
"C:¥Program Files¥Lenovo¥Client Security Solution¥vmserver.exe" /?
```

次の表に、ファイルを処理するためのパラメーターを示します。

表 14. ファイル処理のパラメーター

パラメーター	結果
FILENAME	FILENAME パラメーターにはファイル拡張子 XML または ENC がなければなりません。
PASSPHRASE	PASSPHRASE パラメーターは、拡張子 ENC を持つファイルの暗号化解除に使用します。

例:

```
Vmserver.exe  C:¥DeployScript.xml.enc "my secret"
```

TPMENABLE.EXE

tpmenable.exe ファイルはセキュリティー・チップをオンにしたりオフにするために使用します。

表 15. tpmenable.exe ファイルのパラメーター

パラメーター	説明
/enable または /disable	セキュリティー・チップをオンにしたりオフにしたりします。
/quiet	BIOS パスワードまたはエラーのプロンプトを隠します。
sp:*password*	Windows 2000 および XP の場合に限っては、BIOS 管理者/スーパーバイザー・パスワードは引用符で囲みません。

例:

```
tpmenable.exe /enable /quiet /sp:My BiosPW
```

証明書転送ツール

次の表に、Client Security Solution の証明書転送ツールのコマンド・ライン・スイッチを示します。

表 16. css_cert_transfer_tool.exe <cert_store_type> <filter_type>:<name | size> | all_access | usage

<table>
<tr><th colspan="2">パラメーター</th><th>説明</th></tr>
<tr><td colspan="2"><cert_store_type></td><td>これは最初の必須パラメーターです。最初のスイッチとして使用し、次の例のいずれか 1 つを組み込む必要があります。</td></tr>
<tr><td rowspan="3">例:</td><td>cert_store_user</td><td>ユーザー証明書のみを転送します。ユーザー証明書は、現在のユーザーに割り当てられます。</td></tr>
<tr><td>cert_store_machine</td><td>マシン証明書のみを転送します。マシン証明書は、マシン上で許可されたすべてのユーザーが使用できます。</td></tr>
<tr><td>cert_store_all</td><td>ユーザー証明書タイプとマシン証明書タイプの両方を転送します。</td></tr>
<tr><td colspan="2"><filter_type>:<name | size></td><td>これは 2 番目の必須パラメーターです。必須の <cert_store_type> パラメーターの後に使用する必要があります。各フィルター・タイプ (下記を除く) の後にはコロン「:」が必要で、コロンの直後には、検索対象の証明書所有者の名前、権限、または鍵サイズを指定する必要があります。このユーティリティーは大/小文字の区別があり、検索対象の名前が複合名 (例えば、“CA Authority” など) である場合は、検索条件の前後に二重引用符 “” を使用する必要があります (例を参照)。</td></tr>
</table>

表 16. css_cert_transfer_tool.exe <cert_store_type> <filter_type>:<name | size> | all_access | usage (続き)

パラメーター		説明
例:	subject_simple_name:<name>	証明書の発行先の名前と一致するすべての証明書を転送します。所有者の名前は <name> に指定します。
	subject_friendly_name:<name>	証明書の発行先のフレンドリー名と一致するすべての証明書を転送します。フレンドリー名は <name> に指定します。
	issuer_simple_name:<name>	証明書を発行した証明機関の名前と一致するすべての証明書を転送します。証明機関の名前は <name> に指定します。
	ssuer_friendly_name:<name>	証明書を発行した証明機関のフレンドリー名と一致するすべての証明書を転送します。証明機関のフレンドリー名は <name> に指定します。
	key_size:<size>	鍵サイズ <size> (ビット単位) で暗号化されたすべての証明書を転送します。これは完全一致突き合わせ基準であることに注意してください。プログラムは、そのサイズ以上またはそのサイズ以下の鍵サイズで暗号化された証明書を検索しません。
次の 2 つのスイッチはスタンドアロンです。これらには 2 番目の引数はありません。		
all_access	すべての証明書を転送します。フィルターに掛けないでください。	
usage	コマンド・ラインに関する情報は提供しませんが、正しい使用法を判別するために使用される関数によって、受け渡されたコマンドが正しいかどうかに応じて、true または false が返されます。	

TPM 有効化ツール

tpm_activate_cmd.exe ファイルは、Lenovo システム上で TPM を有効化または無効化するために使用されます。

注: このコマンドを実行するためには、管理者権限が必要です。

表 17. Lenovo システムで TPM を有効化または無効化するためのパラメーター

パラメーター	説明
/help または /?	パラメーターのリストを表示します。
/biospw:*password*	BIOS スーパーバイザーまたは管理者のパスワードが設定されている場合は、それを指定します。
/deactivate	TPM を無効化します。 **注:** パラメーター `/deactivate` を指定して tpm_activate_cmd.exe を実行すると、デフォルトで TPM が有効化されます。
/verbose	テキスト出力を表示します。

例:

```
tpm_activate_cmd.exe /?
tpm_activate_cmd.exe /verbose
tpm_activate_cmd.exe /biospw:pass
```

Active Directory のサポート

Active Directory はディレクトリー・サービスです。ディレクトリーは、ユーザーおよびリソースに関する情報が保存されている場所です。ディレクトリー・サービスによりアクセスが許可されるため、これらのリソースを操作することができます。

Active Directory が提供する機構により、管理者は PC、グループ、ユーザー、ドメイン、セキュリティー・ポリシー、およびすべてのタイプのユーザー定義オブジェクトを管理する機能を得られます。Active Directory がこの機能を付与するために使用する機構のことを、グループ・ポリシーといいます。管理者は、グループ・ポリシーを使用して、PC やユーザーに適用できる設定をドメイン中に定義します。

現在 ThinkVantage テクノロジー製品が使用している、プログラム設定の制御に使用する設定値を収集する方式には、特定のアプリケーション定義レジストリー項目からの読み取りなど、さまざまな方式があります。

以下に、Active Directory が管理できる Client Security Solution の設定の例を示します。

- セキュリティー・ポリシー
- カスタム・セキュリティー・ポリシー (Windows パスワードまたは Client Security Solution パスフレーズを使用するかどうか、など)

管理用 (ADM) テンプレート・ファイル

ADM (管理用) テンプレート・ファイルは、クライアント PC 上のアプリケーションで使用されるポリシー設定を定義します。ポリシーとは、アプリケーションの動作を管理する特定の設定のことです。ポリシー設定は、ユーザーがアプリケーションを使用して特定の設定値を設定できるかどうかも定義します。

サーバー上の管理者が定義する設定は、ポリシーとして定義されます。クライアント PC 上のユーザーが定義する、アプリケーションに関する設定は、プリファレンスとして定義されます。Microsoft 社による定義のとおりに、ポリシー設定はプリファレンスより優先します。

例えば、ユーザーは自分のデスクトップ上に背景イメージを表示することができます。これは、ユーザーのプリファレンス設定です。管理者は、ユーザーが特定の背景イメージを使用しなければならないことを決定する設定をサーバー上で定義できます。管理者のポリシー設定は、ユーザーによるプリファレンス設定をオーバーライドします。

ThinkVantage Technology 製品が設定を確認する際に、次の順序で設定を検索します。

- コンピューター・ポリシー
- ユーザー・ポリシー
- デフォルトのユーザー・ポリシー

- PC プリファレンス
- ユーザー・プリファレンス
- デフォルトのユーザー・プリファレンス

前述のように、コンピューター・ポリシーとユーザー・ポリシーは、管理者によって定義されます。XML 構成ファイルか Active Directory のグループ・ポリシーを使用してこれらの設定値を初期化できます。PC プリファレンスとユーザー・プリファレンスは、クライアント PC 上のユーザーによって、アプリケーション・インターフェース内のオプションを使用して設定されます。デフォルトのユーザー・プリファレンスは、XML 構成スクリプトによって初期化されます。ユーザーは値を直接には変更しません。ユーザーがこれらの設定値に変更を加えるには、ユーザー・プリファレンスを更新します。

Active Directory を使用していないお客様は、クライアント・システムにデプロイされるポリシー設定のデフォルト・セットを作成することができます。管理者は、XML 構成スクリプトを変更して、製品のインストール時にそれらが処理されるように指定することができます。

管理可能設定の定義

この例では、次の階層を使用して、グループ・ポリシー・エディター内に設定を表示します。

```
Computer Configuration>Administrative Templates>ThinkVantage Technologies>
Client Security Solution>Authentication Policies>Max Retries>
Password number of retries
```

ADM ファイルは、レジストリー内の、設定が反映される場所を示します。これらの設定は、レジストリー内の次の場所になければなりません。

```
Computer policies:
HKLM¥Software¥Policies¥Lenovo¥Client Security Solution¥

User policies:
HKCU¥Software¥Policies¥Lenovo¥Client Security Solution¥

Default user policies:
HKLM¥Software¥Policies¥Lenovo¥Client Security Solution¥User defaults

Computer preferences:
HKLM¥Software¥Lenovo¥Client Security Solution¥

User preferences:
HKCU¥Software¥Lenovo¥Client Security Solution¥

Default user preferences:
HKLM¥Software¥Lenovo¥Client Security Solution¥User defaults
```

グループ・ポリシーの設定

このセクションの表には、Client Security Solution の PC 構成およびユーザー構成のポリシー設定が記載されています。

再試行の最大回数

次の表に、「認証ポリシー」の「再試行の最大回数」のポリシー設定を示します。

表 18. コンピュータの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > ThinkVantage > Client Security Solution > Authentication Policies > Max Retries

ポリシー	有効な設定	説明
Password number of retries	再試行の最大回数は 20 です。	ポリシーをオーバーライドする前に、認証のためにユーザーが Windows パスワードを使用できる最大回数を制御します。
Passphrase number of retries	再試行の最大回数は 20 です。	ポリシーをオーバーライドする前に、認証のためにユーザーが Client Security パスフレーズを使用できる最大回数を制御します。

より安全

次の表に、「認証ポリシー」の「保護モード」のポリシー設定を示します。

表 19. コンピュータの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > ThinkVantage > Client Security Solution > Authentication Policies > Secure Mode

ポリシー	有効な設定	説明
Password	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定します。	パスワードが必要であるかどうかを制御します。
Passphrase	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定します。	パスフレーズが必要であるかどうかを制御します。
Fingerprint	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定します。	指紋が必要であるかどうかを制御します。
Override	パスワード、パスフレーズ、または指紋をオーバーライドするように設定します。	通常の認証が失敗した場合の「フォールバック」認証の要件を定義します。

デフォルト・モード

次の表に、「認証ポリシー」の「デフォルト・モード」のポリシー設定を示します。

表 20. コンピュータの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > ThinkVantage > Client Security Solution > Authentication Policies > Default Mode

ポリシー	有効な設定	説明
Password	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定できます。	パスワードが必要であるかどうかを制御します。
Passphrase	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定できます。	パスフレーズが必要であるかどうかを制御します。

表 20. コンピュータの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > ThinkVantage > Client Security Solution > Authentication Policies > Default Mode (続き)

ポリシー	有効な設定	説明
Fingerprint	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定できます。	指紋が必要であるかどうかを制御します。
Smart card	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定できます。	スマート・カードが必要であるかどうかを制御します。
Override	パスワード、パスフレーズ、または指紋をオーバーライドするように設定します。	通常の認証が失敗した場合の「フォールバック」認証の要件を定義します。

認証ポリシー

次のポリシーのリストには、各ポリシーの認証レベルを定義する有効な設定が記載されています。

- Windows logon (Windows へのログオン)
- System unlock (PC のロック解除)
- Password manager (Password Manager を開く)
- CSP signature (CSP シグニチャー)
- CSP decryption (CSP 暗号化解除)
- PKCS#11 signature (PKCS#11 シグニチャー)
- PKCS#11 decryption (PKCS#11 暗号化解除)
- PKCS#11 logon (PKCS#11 ログオン)

次の表に、上記の認証レベルに対する値および設定を示します。

表 21. コンピュータの構成 > 管理用テンプレート > 従来の管理用テンプレート (ADM) > ThinkVantage > Client Security Solution > Authentication Policies

ポリシー	有効な設定	説明
Password	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定します。	パスワードが必要であるかどうかを制御します。
Passphrase	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定します。	パスフレーズが必要であるかどうかを制御します。
Fingerprint	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定します。	指紋が必要であるかどうかを制御します。
Smart card	頻度を「**Every time (毎回)**」または「**Once per logon (ログオンの度に 1 回)**」に設定します。	スマート・カードが必要であるかどうかを制御します。
Override	パスワード、パスフレーズ、または指紋をオーバーライドするように設定します。	通常の認証が失敗した場合の「フォールバック」認証の要件を定義します。

Password Manager

次の表に、Password Manager のポリシー設定を示します。

表 22. コンピュータの構成 > 管理用テンプレート> 従来の管理用テンプレート(ADM) > ThinkVantage > Client Security Solution > Password Manager

ポリシー設定	説明
Disable Password manager	システム始動時に Password Manager が開始するかどうかを制御します。
Disable Internet Explorer support	Password Manager が Internet Explorer からパスワードを保存できるかどうかを制御します。
Disable Mozilla support	Password Manager が Mozilla ベース・ブラウザー (Firefox および Netscape など) からパスワードを保存できるかどうかを制御します。
Disable support for Windows applications	Password Manager が Windows アプリケーションからパスワードを保存できるかどうかを制御します。
Disable Auto-fill	Password Manager が Web サイトおよび Windows アプリケーションへのデータの Auto-fill を行うかどうかを制御します。
Disable Hotkey support	Password Manager が Web サイトおよび Windows アプリケーションにデータを入力するためのホット・キーの使用をサポートするかどうかを制御します。
Use Domain filtering	Password Manager がドメインに基づいて Web サイトをフィルタリングするかどうかを制御します。
Prohibited Domains	Password Manager がパスワードの保存を禁止されているドメインを制御します。
Prohibited URLs	Password Manager がパスワードの保存を禁止されている URL を制御します。
Prohibited Modules	Password Manager がパスワードの保存を禁止されている Windows アプリケーションを制御します。
Auto-fill Hotkey	Auto-fill Hotkey の Ctrl + F2 を制御します。
Type and Transfer Hotkey	Type and Transfer Hotkey の Ctrl + Shift + H を制御します。
Manage Hotkey	ホット・キーの Ctrl + Shift + B を制御します。

ユーザー・インターフェース

次の表に、「ユーザー・インターフェース」のポリシー設定を示します。

表 23. コンピュータの構成> 管理用テンプレート> 従来の管理用テンプレート(ADM) > ThinkVantage > Client Security Solution > User Interface

ポリシー設定	説明
Fingerprint software option	Client Security Solution アプリケーションの指紋認証ソフトウェアのオプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
File encryption option	Client Security Solution アプリケーションのファイル暗号化オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。

表 23. コンピュータの構成> 管理用テンプレート> 従来の管理用テンプレート(ADM) > ThinkVantage > Client Security Solution > User Interface (続き)

ポリシー設定	説明
Security settings audit option	Client Security Solution アプリケーションのセキュリティー設定の監査オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Digital certificate transfer option	Client Security Solution アプリケーションのディジタル証明書の転送オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Change security chip status option	Client Security Solution アプリケーションのセキュリティー・チップの状態オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Clear security chip lockout option	Client Security Solution アプリケーションのセキュリティー・チップのロックアウト・オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Policy manager option	Client Security Solution アプリケーションの Policy manager オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Reset/Configure settings option	Client Security Solution アプリケーションの構成ウィザード・オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Password manager option	Client Security Solution アプリケーションの Password manager オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Hardware Password Reset option	Client Security Solution アプリケーションのハードウェア・パスワードのリセット・オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Windows password recovery option	Client Security Solution アプリケーションの Windows パスワードの復元オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Change authentication mode option	Client Security Solution アプリケーションの認証モードの変更オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Set up smart card option	Client Security Solution アプリケーションのスマート・カードの設定オプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Enable/disable Windows password recovery option	Client Security Solution アプリケーションの、Windows パスワードの復元を有効/無効にするためのオプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。
Enable/disable Password Manager option	Client Security Solution アプリケーションの、Password Manager を有効/無効にするためのオプションを表示するか、ぼかすか、非表示にします。デフォルト: 表示。

ワークステーション・セキュリティー・ツール

次の表に、「ワークステーション・セキュリティー・ツール」のポリシー設定を示します。

表 24. コンピュータの構成> 管理用テンプレート> 従来の管理用テンプレート(ADM) > ThinkVantage > Client Security Solution > Workstation Security Tool

ポリシー	設定	説明
Hardware Passwords	Hardware Passwords	ハードウェア・パスワード情報の表示を有効または無効にします。
Hardware Passwords	Power-On Password	推奨値を有効または無効として選択するか、この設定を無視することを選択します。
Hardware Passwords	Hard Drive Password	推奨値を有効または無効として選択するか、この設定を無視することを選択します。
Hardware Passwords	Administrator Password	推奨値を有効または無効として選択するか、この設定を無視することを選択します。
Windows Users Passwords	Windows Users Passwords	Windows ユーザー・パスワード情報の表示を有効または無効にします。
Windows Users Passwords	Password	推奨値を有効または無効として選択するか、この設定を無視することを選択します。
Windows Users Passwords	Password Age	パスワードが許可される最大日数。
Windows Users Passwords	Password never expires	推奨値を「True」、「False」、または「Ignore」に設定することができます。
Windows Password Policy	Windows Password Policy	Windows パスワード・ポリシー情報の表示を有効または無効にします。
Windows Password Policy	Minimum number of characters in the password	パスワードの最小文字数を指定するか、この値を「無視」します。
Windows Password Policy	Maximum password age	パスワードの最大使用日数 (日数) を設定するか、結果でこの値を「無視」します。
Screen Saver	Screen Saver	Windows パスワード・ポリシー情報の表示を有効または無効にします。
Screen Saver	Screen Saver password set	パスワードの最小文字数を指定するか、この値を「無視」します。
Screen Saver	Screen Saver timeout	パスワードの最大使用日数 (日数) を設定するか、結果でこの値を「無視」します。
File Sharing	File Sharing	ファイル共有情報の表示を有効または無効にします。
File Sharing	Authorized access	推奨値を「True」、「False」、または「Ignore」に設定することができます。
Client Security	Client Security	Client Security 情報の表示を有効または無効にします。
Client Security	Embedded Security Chip	推奨値を有効または無効として選択するか、この設定を無視することを設定します。
Client Security	Client Security Solution Version	Client Security Solution の最小推奨バージョンを設定するか、「Ignore」を設定します。

第 4 章 ThinkVantage 指紋認証ソフトウェアでの作業

指紋コンソールは ThinkVantage 指紋認証ソフトウェア・インストール・フォルダーから実行する必要があります。基本的な構文は FPRCONSOLE [USER | SETTINGS] です。USER コマンドまたは SETTINGS コマンドは、使用する操作モードを指定します。完全なコマンドは「fprconsole user add TestUser」のようになります。コマンドがわからない場合やすべてのパラメーターが指定されていない場合は、短いコマンド・リストがパラメーターと共に表示されます。

ThinkVantage 指紋認証ソフトウェア、インストールの説明、管理コンソール、および関連するすべての資料は、以下の Web サイトで入手できます。
http://www-307.ibm.com/pc/support/site.wss/TVAN-EAPFPR.html

管理コンソール・ツール

このセクションでは、ユーザー固有コマンドとグローバル設定のコマンドに関する情報を提供します。

ユーザー固有コマンド

ユーザーの登録や編集を行う場合は、USER セクションを使用します。現行ユーザーが管理者権限を持っていない場合、コンソールの振る舞いは指紋認証ソフトウェアのセキュリティー・モードによって異なります。保護モード: どのコマンドも許可されません。簡易モード: 標準ユーザーでは、ADD、EDIT、および DELETE コマンドが使用できます。ただし、ユーザーは自分のパスポート (ユーザー名で登録) しか変更できません。構文は次のとおりです。

```
FPRCONSOLE USER command
```

このとき、*command* は次のコマンドの 1 つです:
ADD、EDIT、DELETE、LIST、IMPORT、EXPORT。

表 25. ユーザー固有コマンド

コマンド	構文	説明
新規ユーザーの登録 **Example:** fprconsole user add domain0¥testuser fprconsole user add testuser	ADD [*username* [| *domain¥ username*]]	ユーザー名が指定されない場合は、現行ユーザー名が使用されます。
登録ユーザーの編集 **Example:** fprconsole user edit domain0¥testuser fprconsole user edit testuser	EDIT [*username* [| *domain¥ username*]]	ユーザー名が指定されない場合は、現行ユーザー名が使用されます。 **注:** 登録されるユーザーはまず自分の指紋を検査する必要があります。

表 25. ユーザー固有コマンド (続き)

コマンド	構文	説明

ユーザーの削除
Example:
`fprconsole user delete domain0¥testuser`
 	
`fprconsole user delete testuser`
 	
`fprconsole user delete /ALL`
	`DELETE [`*username* `[|` *domain¥ username* `| /ALL]]`	/ALL フラグは、この PC に登録されているすべてのユーザーを削除します。ユーザー名が指定されない場合は、現行ユーザー名が使用されます。

登録ユーザーの列挙	`List`	登録されたユーザーをリストします。
登録ユーザーのファイルへのエクスポート	`Syntax: EXPORT username [| domain¥username] file`	このコマンドは、登録ユーザーをハードディスクのファイルにエクスポートします。ユーザーは次に、別の PC 上、またはユーザーが削除されている場合は同じ PC 上の IMPORT コマンドを使用してインポートできます。
登録ユーザーのインポート	`Syntax: IMPORT` *file*	このコマンドは指定したファイルからユーザーをインポートします。 **注:** ファイル上のユーザーが同じ指紋を使用してすでに同じ PC に登録されている場合は、識別操作でどちらのユーザーが優先順位を持つかは保証されません。

グローバル設定のコマンド

指紋認証ソフトウェアのグローバル設定は、SETTINGS セクションによって変更できます。このセクションのすべてのコマンドには、管理者権限が必要です。構文は次のとおりです。

```
FPRCONSOLE SETTINGS command
```

このとき、*command* は次のコマンドの 1 つです: SECUREMODE、LOGON、CAD、TBX、SSO。

表 26. グローバル設定のコマンド

コマンド	構文	説明
セキュリティー・モード **Example:** `To set to convenient mode: fprconsole settings securemode 0`	`SECUREMODE 0|1`	この設定は、指紋認証ソフトウェアの簡易モードと保護モードを切り替えます。

表 26. グローバル設定のコマンド (続き)

コマンド	構文	説明
ログオン・タイプ	LOGON 0|1 [/FUS]	この設定は、ログオン・アプリケーションを使用可能 (1)、または使用不可 (0) にします。 /FUS パラメーターを使用する場合、PC の構成上可能であれば、ユーザーの簡易切り替えモードでログオンが可能です。
CTRL+ALT+DEL メッセージ	CAD 0|1	この設定は、ログオンでの「Ctrl+Alt+Delete を押す」テキストを使用可能 (1)、または使用不可 (0) にします。
パワーオン・セキュリティー	TBX 0|1	この設定は、指紋認証ソフトウェアのパワーオン・セキュリティー・サポートをグローバルにオフ (0) にします。パワーオン・セキュリティー・サポートがオフになっている場合は、BIOS 設定に関係なく、パワーオン・セキュリティー・ウィザードやパワーオン・セキュリティー・ページは表示されません。
パワーオン・セキュリティー・シングル・サインオン	SSO 0|1	この設定は、ユーザーが BIOS で検査された際に、自動的にユーザーをログオンさせるための logon で、BIOS で使用される指紋を使用可能 (1)、または使用不可 (0) にします。

保護モードおよび簡易モード

指紋認証ソフトウェアは、保護モードと簡易モードの 2 つのセキュリティー・モードで実行することができます。保護モードは、より高レベルのセキュリティーが必要な状況を対象としています。特定の機能は管理者にのみ、確保されています。追加認証をせず、パスワードを使用してログオンできるのは管理者だけです。

簡易モードは高レベルのセキュリティーをそれほど重要視しない、家庭用 PC を対象にしています。すべてのユーザーは、他のユーザーのパスポートの編集およびパスワードを使用して (指紋認証は行わない) システムにログオンするなどの、すべての操作を実行できます。

管理者 は、ローカル管理者グループの任意のメンバーです。保護モードを設定した後は、管理者だけが簡易モードに切り替えることができます。

保護モード - 管理者

セキュリティーを強化するために、ログオンのとき、誤ったユーザー名やパスワードが入力された場合は、保護モードでは次のメッセージが表示されます。「ユーザ

ー名とパスワードでこの PC にログオンできるのは管理者だけです。」

表 27. 保護モードでの管理者用オプション

指紋	**説明**
新規パスポートの作成	管理者は自分のパスポートを作成することができ、また、制限ユーザーのパスポートも作成することができます。
パスポートの編集	管理者は自分のパスポートだけ を編集できます。
パスポートの削除	管理者はすべての制限ユーザーとその他の管理者のパスポートを削除できます。他のユーザーがパワーオン・セキュリティーを使用している場合、管理者はパワーオン・セキュリティーからユーザー・テンプレートをオプションで削除することができます。
パワーオン・セキュリティー	管理者は、パワーオンで使用される制限ユーザーおよび管理者の指紋を削除することができます。 **注:** パワーオン・モードが使用可能な場合は、少なくとも 1 つの指紋がなければなりません。
設定	
ログオン設定	管理者はすべてのログオン設定を変更できます。
保護スクリーン・セーバー	管理者はアクセスできます。
パスポート・タイプ	管理者はアクセスできます - サーバーと関連ある場合のみです。
セキュリティー・モード	管理者は保護モードと簡易モードを切り替えることができます。
Pro サーバー	管理者はアクセスできます - サーバーと関連ある場合のみです。

保護モード - 制限ユーザー

Windows にログオン中は、制限ユーザーはログオンに指紋を使用する必要があります。制限ユーザーの指紋センサーが作動していない場合は、管理者は指紋認証ソフトウェアの設定を簡易モードに変更して、ユーザー名とパスワードによるアクセスを可能にする必要があります。

表 28. 保護モードでの制限ユーザー用オプション

設定	**説明**
新規パスポートの作成	制限ユーザーはアクセスできません。
パスポートの編集	制限ユーザーは自分のパスポートだけを編集できます。
パスポートの削除	制限ユーザーは自分のパスポートだけを削除できます。
パワーオン・セキュリティー	制限ユーザーはアクセスできません。

表 28. 保護モードでの制限ユーザー用オプション (続き)

設定	説明
ログオン設定	制限ユーザーはログオン設定を変更できません。
保護スクリーン・セーバー	制限ユーザーはアクセスできます。
パスポート・タイプ	制限ユーザーはアクセスできません。
セキュリティー・モード	制限ユーザーはセキュリティー・モードを変更できません。
Pro サーバー	制限ユーザーはアクセスできます - サーバーと関連ある場合のみです。

簡易モード - 管理者

Windows へのログオン中は、管理者はユーザー名とパスワードを使用しても、指紋を使用してもログオンできます。

表 29. 簡易モードでの管理者用オプション

設定	説明
新規パスポートの作成	管理者は自分のパスポートだけ を作成できます。
パスポートの編集	管理者は自分のパスポートだけ を編集できます。
パスポートの削除	管理者は自分のパスポートだけ を削除できます。
パワーオン・セキュリティー	管理者は、パワーオンで使用される制限ユーザーおよび管理者の指紋を削除することができます。 **注:** パワーオン・モードが使用可能な場合は、少なくとも 1 つの指紋がなければなりません。
ログオン設定	管理者はすべてのログオン設定を変更できます。
保護スクリーン・セーバー	管理者はアクセスできます。
パスポート・タイプ	管理者はアクセスできます - サーバーと関連ある場合のみです。
セキュリティー・モード	管理者は保護モードと簡易モードを切り替えることができます。
Pro サーバー	管理者はアクセスできます - サーバーと関連ある場合のみです。

簡易モード - 制限ユーザー

Windows へのログオン中は、制限ユーザーはユーザー名とパスワードを使用しても、指紋を使用してもログオンできます。

表 30. 簡易モードでの制限ユーザー用オプション

設定	説明
新規パスポートの作成	制限ユーザーは自分のパスワードだけを作成できます。
パスポートの編集	制限ユーザーは自分のパスポートだけを編集できます。
パスポートの削除	制限ユーザーは自分のパスポートだけを削除できます。
パワーオン・セキュリティー	制限ユーザーは自分の指紋だけを削除できます。
ログオン設定	制限ユーザーはログオン設定を変更できません。
保護スクリーン・セーバー	制限ユーザーはアクセスできます。
パスポート・タイプ	制限ユーザーはアクセスできません - サーバーと関連ある場合のみです。
セキュリティー・モード	制限ユーザーはセキュリティー・モードを変更できません。
Pro サーバー	制限ユーザーはアクセスできます - サーバーと関連ある場合のみです。

構成可能な設定

指紋認証ソフトウェアの一部のオプションはレジストリー設定で構成することができます。

- **起動前/パワーオン時ソフトウェア・インターフェース**: 指紋の起動前またはパワーオン時サポートを有効にし、指紋をコンパニオン・チップに格納するための機構は、システムに BIOS またはハードディスク・パスワードが設定されていない限り、通常は指紋認証ソフトウェアに表示されません。この動作をオーバーライドし、BIOS またはハードディスク・パスワードが設定されていなくてもこれらのオプションを強制的に表示させるには、レジストリーに以下のいずれか (使用しているコンピューター・マシン・タイプに適用されるもの) を追加します。

  ```
  [HKEY_LOCAL_MACHINE¥SOFTWARE¥Protector Suite QL¥1.0]

  REG_DWORD "BiosFeatures" = 2
  ```

  または

  ```
  [HKEY_LOCAL_MACHINE¥SOFTWARE¥Protector Suite QL¥1.0]

  REG_DWORD "BiosFeatures" = 4
  ```

  この設定は、BIOS パスワードが設定されていないシステムに SafeGuard Easy がインストールされ、その SafeGuard Easy がハードディスクを暗号化解除するのに指紋認証を利用している場合に役立ちます。

- **音**: 指紋認証ソフトウェアは、指紋認証プロセスの実行中のさまざまな状況下において、.wav ファイルに含まれる音を再生するように構成できます。これらの音のレジストリー設定は次のとおりです。

```
[HKEY_LOCAL_MACHINE¥SOFTWARE¥Protector Suite QL¥1.0¥settings]
'Success'
REG_SZ "sndSuccess" = [path to sound file]
The file designated will play whenever a successful swipe is registered.

'Failure'
REG_SZ "sndFailure" = [path to sound file]
The file designated will play whenever an unsuccessful swipe is attempted.

HKEY_LOCAL_MACHINE¥SOFTWARE¥Policies¥fingerprint

'Scan'
REG_SZ "sndScan" = [path to sound file]
The file designated will play whenever the fingerprint verification
 dialog is displayed for Client Security Solution-related operations.
If the value is not present or is empty then no sound is played.

'Quality'
REG_SZ "sndQuality" = [path to sound file]
The file designated will play whenever an unreadable swipe has occurred.
If the value is not present or is empty then no sound is played.
```

- **システム・ロック解除中のパスワードの有効性検証**: デフォルトでは、システム・ロック解除中には、保存されているパスワードが指紋認証ソフトウェアによって有効性が検証されます。有効性検証では、ドメイン・コントローラーと連絡を取る必要があり、遅延が生じる可能性があります。遅延を回避するには、システム・ロック解除中に次のようにレジストリーを編集して、パスワードの有効性検証を無効にします。

  ```
  [HKEY_LOCAL_MACHINE¥SOFTWARE¥Protector Suite QL¥1.0¥settings]
  REG_DWORD "DoNotTestUnlock"=1
  ```

  指紋認証ソフトウェアはシステム・ログオン時には、引き続きパスワードの有効性を検証します。

  注: 上記のレジストリー・キーを 1 に設定すると、ドメイン管理者がユーザーのシステムをロックする時期を変更した場合は、ユーザーがログオフして再度ログオンするまで、指紋認証ソフトウェアには旧パスワードが保存されます。

指紋認証ソフトウェアおよび Novell Netware Client

競合を防止するために、指紋認証ソフトウェアおよび Novell NetWare Client のユーザー名とパスワードは一致する必要があります。お使いの PC に指紋認証ソフトウェアがインストールしてあり、Novell Netware Client をインストールする場合は、レジストリーの一部の項目が上書きされることがあります。指紋認証ソフトウェアのログオンで問題が発生した場合は、ログオン設定画面に移動して、ログオン・プロテクターを再度使用可能にしてください。

お使いの PC に Novell Netware Client がインストールされていても、指紋認証ソフトウェアのインストール前にクライアント PC にログオンしていなかった場合、Novell のログオン画面が表示されます。画面で、必要な情報を入力してください。

注: このセクションの情報は ThinkVantage 指紋認証ソフトウェア専用です。

ログオン・プロテクター設定を変更するには、次のようにします。

- 「コントロールセンター」を開始する。
- 「**設定**」をクリックする。
- 「**ログオン設定**」をクリックする。
- ログオン・プロテクターを使用可能または使用不可にする。

  指紋ログオンを使用したい場合は、「Windows ログオン認証を通常のパスワード認証から指紋認証に置き換える」チェック・ボックスにチェック・マークを付けます。

  注: ログオン・プロテクターを使用可能、または使用不可にするには、再起動が必要です。
- お使いのシステムでユーザーの簡易切り替えがサポートされている場合は、これを使用可能または使用不可にする。
- (オプション機能) パワーオン・セキュリティーによって認証されたユーザーの自動ログオンを使用可能または使用不可にする。
- Novell ログオン設定を設定する。Novell ネットワークにログオンする場合は、次の設定が使用可能です。
  - **活動化**

    指紋認証ソフトウェアは自動的に既知のクレデンシャルを提供します。 Novell のログオンが失敗すると、Novell Client ログオン画面が表示され、正しいデータの入力を要求するプロンプトが出されます。
  - **ログオン中の質問**

    指紋認証ソフトウェアは Novell Client ログオン画面を表示して、ログオン・データの入力を要求するプロンプトを出します。
  - **使用不可**

    指紋認証ソフトウェアは Novell ログオンを試行しません。

認証

Novell を指紋認証ソフトウェアに引き渡すには、次のステップを実行します。

1. 指紋認証ソフトウェアをインストールする。
2. Novell Netware Client をインストールする。
3. プロンプトが出されたら、「**はい**」をクリックしてログオンする。
4. 再起動する。
5. プロンプトが出されたら、「はい」をクリックして指紋認証ソフトウェアにログオンする。
6. Novell Netware Client を起動する。
7. サーバーに対して認証を行う。
8. Windows にログオンする。
9. 再起動する。

注: Windows と Novell の認証 ID およびパスワードは同じでなければなりません。

ThinkVantage 指紋認証ソフトウェアのサービス

ThinkVantage 指紋認証ソフトウェアのインストール後、upeksvr.exe サービスがシステムに追加されます。起動中に実行が開始されて、ユーザーがログオンしている間中、実行が続けられます。upeksvr.exe サービスは、ThinkVantage 指紋認証ソフトウェアのコアで、デバイスとユーザーのデータに対してすべての操作を実行します。また、すべての生体測定検査の GUI を提供し、ユーザーのデータに対するアクセスをセキュアにします。

第 5 章 Lenovo Fingerprint Software での作業

指紋コンソールは、Lenovo Fingerprint Software インストール・フォルダーから実行する必要があります。基本的な構文は FPRCONSOLE [USER | SETTINGS] です。USER コマンドまたは SETTINGS コマンドは、どの操作セットを使用するかを指定します。完全なコマンドは「fprconsole user add TestUser」のようになります。コマンドがわからない場合やすべてのパラメーターが指定されていない場合は、短いコマンド・リストがパラメーターと共に表示されます。

Lenovo Fingerprint Software、インストールの説明、管理コンソール、および関連するすべての資料は、以下の Lenovo Web サイトで入手できます。
http://www.lenovo.com/support

管理コンソール・ツール

Lenovo Fingerprint Software の管理コンソール・ツールについては、59 ページの『管理コンソール・ツール』を参照してください。

Lenovo Fingerprint Software のサービス

注: Lenovo Fingerprint Software は、システム上のターミナル・サービスを必要とします。ターミナル・サービスをオフにすると、Lenovo Fingerprint Software で予期しない結果が生じる可能性があります。

Lenovo Fingerprint Software のインストール後、以下のサービスがシステムに追加されます。

- ATService.exe (デフォルトでオン)

  指紋認証システムを使用するには、ATService.exe サービスをオンにする必要があります。このサービスは、指紋センサーを使用してアプリケーションからの要求を管理します。

- データ転送サービス (デフォルトでオン)

  データ転送サービスまたは ATService.exe サービスが異常終了する場合、Lenovo Fingeprint Software は予期どおりに動作しません。

- ADMonitor.exe (デフォルトでオフ)

  Active Directory 管理をサポートするには、ADMonitor.exe サービスをオンにする必要があります。このサービスは、Active Directory から伝搬された変更がないかレジストリーをモニターし、ローカルでその変更を反映させます。

Lenovo Fingerprint Software の Active Directory サポート

次の表に、Lenovo Fingerprint Software のポリシー設定を示します。

表 31. ポリシー設定

設定	説明
Enable/disable fingerprint logon	コンピューターにログインするために Windows パスワードではなく、指紋を使用するように指定します。 これを使用可能に設定した場合、さらに使用可能または使用不可に設定できる 2 つのオプションがあります。 • **Disable CTRL+ALT+DEL dialog for logon interface** このオプションを選択すると、ユーザーに Ctrl+Alt+Delete を押してログインするように指示するメッセージがオフになります。(Windows XP でのみ使用可能です) • **Require non-administrator user logon with fingerprint authentication** このオプションを選択した場合、管理者以外のユーザーは、指紋を使用したログインのみが可能になります。
Allow user to retrieve password through fingerprint authentication	これを使用可能に設定した場合、ユーザーは、指紋認証後に、Lenovo Fingerprint Software でユーザーのアカウントの Windows パスワードを表示できます。
Always show power-on security options	これを使用可能に設定した場合、コンピューターがオンになったとき、ユーザーは、パワーオン・パスワードとハードディスク・ドライブ・パスワードではなく指紋センサーを使用するように選択できます。Lenovo Fingerprint Software の登録ウィンドウで、登録する各指ごとに、パワーオン指紋認証を使用可能または使用不可に設定できます。
Use fingerprint authentication instead of power-on and HD passwords	これを使用可能に設定すると、パワーオンおよびハードディスク・ドライブのパスワードではなく、指紋認証が使用されます。
Set number of failed attemps before lock out	ユーザーがロックアウトされる前に許可するログオン試行失敗の数を設定し、ユーザーがロックアウトされる期間 (秒単位) も設定します。
Set inactive timeout	ユーザーがログオフするまでに許可されるシステムの非活動期間 (秒単位) を設定します。
Allow users to enroll fingerprints	これを使用可能に設定した場合、管理者以外のユーザーは、Lenovo Fingerprint Software を使用して指紋を登録できます。

表 31. ポリシー設定 (続き)

設定	**説明**
Allow users to delete fingerprints	これを使用可能に設定した場合、管理者以外のユーザーは、Lenovo Fingerprint Software を使用して、以前に登録した指紋を削除できます。
Allow users to import/export fingerprints	これを使用可能に設定した場合、管理者以外のユーザーは、Lenovo Fingerprint Software を使用して、以前に登録した指紋をインポートおよびエクスポートできます。
Show/Hide elements in setting tab of fingerprint software	これを使用可能に設定した場合、IT 管理者は、指紋認証ソフトウェアの設定 GUI を制御できます。

第 6 章 ベスト・プラクティス

この章では、Client Security Solution および指紋認証ソフトウェアのベスト・プラクティスを示すシナリオを提示します。このシナリオでは、ハードディスク・ドライブの設定から始まり、何回かの更新を行い、デプロイメントまでの手順を説明しています。 Lenovo および他社製の両方の PC でのインストールを説明します。

Client Security Solution をインストールする場合のデプロイメント例

次のセクションでは、Client Security Solution をデスクトップとノートブック・コンピューターの両方にインストールする場合の例をいくつか挙げます。

シナリオ 1

これは、各製品を次のような仮定のカスタマー要件でデスクトップ PC にインストールする場合の例です。

- **Administration**

  PC の管理にローカル管理者アカウントを使用
- **Client Security Solution**
  - エミュレーション・モードでのインストールおよび実行

    Lenovo の PC すべてが TPM (セキュリティー・チップ) を備えているわけではありません。
  - Client Security パスフレーズを使用可能に設定

    パスフレーズによって Client Security Solution アプリケーションを保護します。
  - Client Security Windows ログオンを使用可能に設定

    Client Security パスフレーズで Windows にログインします。
  - エンド・ユーザー・パスフレーズのリカバリー機能を使用可能に設定

    ユーザーが、自分で決めた 3 つの質問に答えることによって、パスフレーズを復元できるようにします。
  - パスワード (XMLscriptPW など) を使用した Client Security Solution XML スクリプトの暗号化

    Client Security Solution 構成ファイルをパスワードで保護します。
  - 指紋認証ソフトウェアのインストールはオプション

準備マシンで以下を実行します。

1. ローカル管理者アカウントで Windows にログインします。
2. Client Security Solution を、次のコマンドを使用してインストールします。

   ```
   tvtcss83_xxxx.exe /s /v"/qn "EMULATIONMODE=1" "NOCSSWIZARD=1"
   ```

   (where *XXXX* is the build ID)
3. コンピューターを再起動し、ローカル管理者アカウントを使用して Windows にログインします。
4. 以下を実行して、デプロイメント用の XML スクリプトを作成します。
   a. 次のコマンドを実行します。

      ```
      "C:¥Program Files¥Lenovo¥Client Security Solution¥css_wizarde.exe"
      /name:C:¥ThinkCentre
      ```

   b. 以下を実行して、ウィザードで構成を行います。
      1) 「**セキュア・ログオン・メソッド**」 → 「**次へ**」をクリックします。
      2) 管理者アカウント用の Windows パスワード (`WPW4Admin` など) を入力して、「**次へ**」をクリックします。
      3) 管理者アカウント用の Client Security パスフレーズ (`CSPP4Admin` など) を入力して、「**Client Security パスフレーズを使用して、Rescue and Recovery ワークスペースへのアクセスを保護する**」オプションを選択してから、「**次へ**」をクリックします。
      4) 管理者アカウント用の 3 つの質問に答えてから、「**次へ**」をクリックします。質問の例を以下に記します。
         a) 初めて飼ったペットの名前は?
         b) 好きな映画は?
         c) 好きなスポーツ・チームは?
      5) 要約を確認し、「**適用**」を選択して、XML ファイルを次の場所に保存します。
         C:¥ThinkCentre.xml
      6) 「**完了**」をクリックしてウィザードを閉じます。
5. テキスト・エディター (XML スクリプト・エディター、または XML 形式をサポートしている Microsoft Word 2003 プログラム) で ThinkCentre.xml ファイルを開いて、ドメイン設定へのすべての参照を除去してから、ファイルを保存します。これにより、スクリプトは、各システムで代わりにローカル・マシン名を使用します。
6. C:¥Program Files¥Lenovo¥Client Security Solution ディレクトリーの xml_crypt_tool.exe ツールを使用して、XML スクリプトをパスワードで暗号化します。その際、以下の構文を使用します。

   ```
   xml_crypt_tool.exe C:¥ThinkCentre.xml /encrypt XMLScriptPW
   ```

   これでファイルは C:¥ThinkCentre.xml.enc となり、パスワード `XMLScriptPW` で保護され、デプロイメント・マシンに追加する準備が整いました。

デプロイメント・マシンで以下を実行します。

1. ローカル管理者アカウントで Windows にログインします。
2. Rescue and Recovery および Client Security Solution を、次の構文でインストールします。

   ```
   setup_tvtrnr40_xxxxcc.exe /s /v"/qn "EMULATIONMODE=1" "NOCSSWIZARD=1"
   ```

   (ここで *xxxx* はビルド ID で、*cc* は国別コードです。)

   注:

   a. Windows XP では Z652ZIXxxxxyy00.tvt、Windows Vista または Windows 7 では Z633ZISxxxxyy00.tvt (xxxx はビルド ID、yy は国 ID です) などの TVT ファイルが実行可能ファイルと同じディレクトリーにあることを確認します。同じディレクトリーにない場合、インストールは失敗します。

   b. 管理者用インストールを実行する場合は、 73 ページの『シナリオ 1』を参照してください。
3. コンピューターを再起動し、ローカル管理者アカウントを使用して Windows にログインします。
4. 先に作成した ThinkCentre.xml.enc ファイルを C:¥ のルート・ディレクトリーに追加します。
5. RunOnceEx コマンドを、以下のパラメーターを指定して作成します。

   a. RunonceEx キーの後に 0001 という新規キーを追加します。次のようになります。

   ```
   HKEY_LOCAL_MACHINE ¥Software¥Microsoft¥Windows
   ¥Current Version¥RunOnceEx¥0001
   ```

   b. このキーに CSSEnroll というストリング値名を追加します。

   ```
   "C:¥Program Files¥Lenovo¥Client Security Solution¥vmserver.exe"
   C:¥ThinkCenter.xml.enc XMLscriptPW
   ```
6. 以下のコマンドを実行して、sysprep バックアップ用にシステムを準備します。

   ```
   %rr%C:¥Program Files¥Lenovo¥Rescue and Recovery¥rrcmd.exe"
   sysprepbackup location=L name="Sysprep Backup"
   ```

   その後、システムで sysprep バックアップを行う準備が整うと以下の出力が表示されます。

   ```
   *******************************************************
   ** Ready to take sysprep backup.                     **
   **                                                   **
   ** PLEASE RUN SYSPREP NOW AND SHUT DOWN.             **
   **                                                   **
   ** Next time the machine boots, it will boot         **
   ** to the Predesktop Area and take a backup.         **
   *******************************************************
   ```
7. Sysprep を実行します。
8. シャットダウンしてから、コンピューターを再起動します。Rescue and Recovery ワークスペースで、バックアップ処理が開始されます。

   注: 「復元が進行中ですが、バックアップが行われています」というメッセージが表示される場合、バックアップ後にコンピューターをシャットダウンし、再起動はしないでください。
9. これで、Sysprep の基本バックアップが完了しました。

シナリオ 2

これは、各製品を次のような仮定のカスタマー要件でノートブック・コンピューターにインストールする場合の例です。

- **Administration**
  - 旧バージョンの Client Security Solution がインストールされているマシンにインストール
  - PC の管理にドメイン管理者アカウントを使用
  - すべてのコンピューターに、BIOS スーパーバイザー・パスワード `BIOSpw` を割り当て
- **Client Security Solution**
  - TPM を活用

    すべてのマシンにセキュリティー・チップを搭載
  - Password Manager を使用可能に設定
  - Client Security Solution に対する認証として、ユーザーの Windows パスワードを活用
  - パスワード (XMLscriptPW など) を使用した Client Security Solution XML スクリプトの暗号化

    Client Security Solution 構成ファイルをパスワードで保護します。
- **ThinkVantage 指紋認証ソフトウェア**
  - BIOS とハードディスク・ドライブのパスワードを使用しない
  - ThinkVantage 指紋認証ソフトウェアを使用して Windows にログインする

    一定のセルフ・ユーザー登録期間後、ユーザーは、管理者以外のユーザーの場合は指紋を必要とする保護モード・ログオンに切り替えて、デュアル・ファクター認証方式を効果的に実行できます。
  - 指紋認証ソフトウェア・チュートリアルの組み込み

    指紋認証ソフトウェア・チュートリアルは、エンド・ユーザーが、指紋センサーで指紋を読み取る方法について理解を深め、そのアクションの視覚的フィードバックを確認するのに役立ちます。

準備マシンで以下を実行します。

1. 電源オフの状態からコンピューターを始動し、**F1** を押して BIOS Setup Utility に入り、「**Security**」メニューに移動してセキュリティー・チップをクリアします。設定を保存して、BIOS を終了します。
2. ドメイン管理者アカウントで Windows にログインします。
3. 以下を実行して、ThinkVantage 指紋認証ソフトウェアをインストールします。
   a. f001zpz2001us00.exe ファイルを実行して、Web パッケージから setup.exe ファイルを解凍します。setup.exe ファイルが、以下の場所に自動的に解凍されます。
   C:¥SWTOOLS¥APPS¥TFS5.9.2-Buildxxxx¥Application¥0409 (ここで xxxx はビルド ID です)。

b. 解凍された setup.exe ファイルをダブルクリックして、画面上の指示に従って、ThinkVantage 指紋認証ソフトウェアをインストールします。

4. 以下を実行して、ThinkVantage 指紋認証ソフトウェア・チュートリアルをインストールします。

 a. f001zpz7001us00.exe ファイルを実行して、Web パッケージから tutess.exe ファイルを解凍します。tutess.exe ファイルが、以下の場所に自動的に解凍されます。

 C:¥SWTOOLS¥APPS¥tutorial¥TFS5.9.2 Buildxxxx¥Tutorial¥0409 (ここで xxxx はビルド ID です)。

 b. tutess.exe ファイルをダブルクリックして、ThinkVantage 指紋認証ソフトウェア・チュートリアルをインストールします。

5. 以下を実行して、ThinkVantage 指紋認証コンソールをインストールします。

 a. f001zpz5001us00.exe を実行して、Web パッケージから fprconsole.exe ファイルを解凍します。fprconsole.exe ファイルが、以下の場所に自動的に解凍されます。

 C:¥SWTOOLS¥APPS¥fpr_con¥APPS¥UPEK¥FPR Console¥TFS5.9.2-Buildxxx¥Fprconsole (ここで xxxx はビルド ID です)。

 b. fprconsole.exe ファイルをダブルクリックして、ThinkVantage 指紋認証コンソールをインストールします。

6. Client Security Solution を、次の構文でインストールします。

```
tvtcss82_xxxxcc.exe /s /v"/qn NOCSSWIZARD=1 SUPERVISORPW="BIOSpw""
```

7. コンピューターを再起動し、ドメイン管理者アカウントを使用して Windows にログインし、デプロイメント用の XML スクリプトを作成します。

 a. 次のコマンドを実行します。

```
"C:¥Program Files¥Lenovo¥Client Security Solution¥css_wizard.exe"
/name:C:¥ThinkPad
```

 b. 以下を実行して、スクリプト例に合わせてウィザードで構成を行います。

  1) 「**セキュア・ログオン・メソッド**」 → 「**次へ**」をクリックします。

  2) ドメイン管理者アカウント用の Windows パスワード (`WPW4Admin` など) を入力して、「**次へ**」をクリックします。

  3) ドメイン管理者アカウントの Client Security パスフレーズを入力します。

  4) 「**パスワード復元を無効に設定**」を選択してから、「**次へ**」をクリックします。

  5) 要約を確認し、「**適用**」をクリックして、XML ファイルを次の場所に保存します。

  C:¥ThinkPad.xml

  6) 「**完了**」をクリックしてウィザードを閉じます。

8. C:¥Program Files¥Lenovo¥Client Security Solution ディレクトリーの xml_crypt_tool.exe ツールを使用して、次のように XML スクリプトをパスワードで暗号化します。
コマンド・プロンプトで、次の構文を使用します。

```
xml_crypt_tool.exe C:¥ThinkPad.xml /encrypt XMLScriptPW
```

これでファイルは C:¥ThinkPad.xml.enc となり、パスワード XMLScriptPW で保護されます。

デプロイメント・マシンで以下を実行します。

1. 以下を実行して、ThinkVantage 指紋認証ソフトウェアをデプロイメント・マシンにインストールします。
   a. 準備マシンから取り出した setup.exe ファイルをデプロイメント・マシンにデプロイします。その際、自社のソフトウェア配布ツールを使用します。
   b. 次のコマンドを実行します。
   ```
   setup.exe CTLCNTR=0 /q /i
   ```
2. 以下を実行して、ThinkVantage 指紋認証ソフトウェア・チュートリアルをデプロイメント・マシンにインストールします。
   a. 準備マシンから取り出した tutess.exe ファイルをデプロイメント・マシンにデプロイします。その際、自社のソフトウェア配布ツールを使用します。
   b. 次のコマンドを実行します。
   ```
   tutess.exe /q /i
   ```
3. 以下を実行して、ThinkVantage 指紋認証コンソールをデプロイメント・マシンにインストールします。
   a. 準備マシンから取り出した fprconsole.exe ファイルをデプロイメント・マシンにデプロイします。その際、自社のソフトウェア配布ツールを使用します。
   b. fprconsole.exe ファイルを C:¥Program Files¥ThinkVantage Fingerprint Software ディレクトリーに入れます。
   c. 次のコマンドを実行して、BIOS パワーオン・セキュリティー・サポートをオフにします。
   ```
   fprconsole.exe settings TBX 0
   ```
4. 以下を実行して、ThinkVantage Client Security Solution をデプロイメント・マシンにインストールします。
   a. tvtvcss83_xxxx.exe (ここで *xxxx* はビルド ID です) ファイルを、デプロイメント・マシンにデプロイします。その際、自社のソフトウェア配布ツールを使用します。
   b. 次のコマンドを実行します。
   ```
   tvtvcss83_xxxx.exe /s /v"/qn "NOCSSWIZARD=1" "SUPERVISORPW="BIOSpw""
   ```
   ソフトウェアをインストールすると、 TPM ハードウェアが自動的に使用可能になります。
5. コンピューターを再起動し、次の手順で、XML スクリプト・ファイルによるシステム構成を行います。
   a. 先に作成した ThinkPad.xml.enc ファイルを、C:¥ フォルダーにコピーします。
   b. 次のコマンドを実行します。
   ```
   "C:¥Program Files¥Lenovo¥Client Security Solution¥
   vmserver.exe" C:¥ThinkPad.xml.enc XMLScriptPW
   ```
6. コンピューターを再起動すると、システムで Client Security Solution ユーザー登録の準備ができています。すべてのユーザーは、それぞれのユーザー ID と

Windows パスワードでシステムにログインできます。システムにログインする各ユーザーに、Client Security Solution への登録を促すプロンプトが自動的に出され、登録すると、指紋センサーへの登録ができるようになります。

7. システムのすべてのユーザーが ThinkVantage 指紋認証ソフトウェアに登録されたら、保護モード設定を使用可能にして、Windows のすべての管理者以外のユーザーに、各自の指紋でログインするよう求めることができます。
   - 保護モード設定を使用可能にするには、次のコマンドを実行します。
     ```
     "C:¥Program Files¥ThinkVantage Fingerprint Software¥
     fprconsole.exe" settings securemode 1
     ```
   - 「パスワードを使用してログインするには Ctrl+Alt+Delete を押してください (Press Ctrl+Alt+Delete to log in using a password)」というメッセージをログオン画面から削除するには、次のコマンドを実行してください。
     ```
     "C:¥Program Files¥ThinkVantage Fingerprint Software¥fprconsole.exe settings"
     CAD 0
     ```
8. これで、Client Security Solution 8.3 と ThinkVantage 指紋認証ソフトウェアのデプロイメントが完了しました。

Client Security Solution モードの切り替え

Client Security Solution モードを「便利なログオン・メソッド」から「セキュア・ログオン・メソッド」に切り替えるか、「セキュア・ログオン・メソッド」から「便利なログオン・メソッド」に切り替える場合で、システムのバックアップに Rescue and Recovery を使用している場合、モードを切り替えた後に新しい基本バックアップをとってください。

企業用 Active Directory の展開

企業用 Active Directory を展開する場合、次のステップを実行します。

1. Active Directory または LANDesk を使用してインストールします。
   a. Active Directory および LANDesk を使用してバックアップを取り、バックアップを取った人物と時点について報告を得ます。
   b. バックアップの作成、バックアップの削除、スケジュール・オプション、およびパスワードの制約事項に関する機能を特定のグループに付与してから、グループを変更し、設定が存続するかどうかを参照します。
   c. Active Directory から Antidote Delivery Manager を有効にします。実行するパッケージを提供し、報告が取り込まれることを確認します。

CD またはスクリプト・ファイルのスタンドアロン・インストール

CD またはスクリプト・ファイルのスタンドアロン・インストールの場合、次のステップを実行します。

1. バッチ・ファイルを使用して Client Security Solution および指紋認証ソフトウェア・テクノロジーをサイレント・インストールします。
2. BIOS パスワード・リカバリーをサイレント構成します。

System Update

System Update をするには、次のステップを実行します。

1. Lenovo サーバーを使う代わりに、大企業がサーバーをセットアップする方法をシミュレートしたカスタマイズ済みの System Update サーバーを使って Client Security Solution および指紋認証ソフトウェアをインストールすれば、コンテンツの管理ができます。
2. 3 種類のバージョンの古いソフトウェア (Rescue and Recovery 1.0/2.0/3.0、指紋認証、Client Security Solution 5.4-6、FFE) を上書きインストールします。古いバージョンに上書きして新しいバージョンをインストールする際には、設定を保持する必要があります。

System Migration Assistant

System Migration Assistant 6.0 は、古いシステムから最新の Windows 7 システムへの移行、および旧バージョンの Client Security Solution と指紋認証ソフトウェアのソフトウェア設定の移行をサポートしています。System Migration Assistant 6.0 は、以下の Lenovo Web サイトからダウンロードできます。

http://www.lenovo.com/support

TPM での鍵生成を使用した証明書の生成

証明書は Client Security Solution CSP を使用して直接生成でき、証明書内の秘密鍵は TPM によって生成され、保護されます。 Client Security Solution CSP を使用して証明書を要求するには、次のようにします。

要件:

- サーバー・マシンに以下がインストールされている必要があります。
  - Windows Server 2003 Enterprise 以上
  - Active Directory
  - 証明機関サービス
- クライアント・マシンは以下の要件に適合している必要があります。
  - TPM が使用可能になっている
  - Client Security Solution がインストールされている

サーバーからの証明書の要求

TPM ユーザーのテンプレートの作成

TPM ユーザー用のテンプレートを作成するには、以下の手順を実行します。

1. 「**スタート**」 → 「**ファイル名を指定して実行**」をクリックします。
2. mmc と入力し、「**OK**」をクリックします。コンソール・ウィンドウが表示されます。
3. 「**ファイル**」メニューの「**スナップインの追加と削除**」をクリックしてから、「**追加**」をクリックします。「スタンドアロン スナップインの追加」ウィンドウが表示されます。

4. スナップイン・リストで「**証明機関 (Certification Authority)**」をダブルクリックし、「**閉じる**」をクリックします。
5. 「スナップインの追加と削除」ウィンドウで「**OK**」をクリックします。
6. コンソール・ツリーから「**証明書テンプレート**」をクリックします。すべての証明書テンプレートが左側のペインに表示されます。
7. 「**操作**」 → 「**テンプレートの複製**」をクリックします。
8. 「**表示名**」フィールドに TPM User と入力します。
9. 「**要求処理**」タブで「**CSP**」をクリックします。「**サブジェクトのコンピュータで利用可能な任意の CSP (Requests can use any CSP available on the subject's computers)**」が選択されていることを確認します。
10. 「**全般**」タブをクリックします。「**Active Directory の証明書を発行する**」が選択されていることを確認します。
11. 「**グループ名またはユーザー名**」リストの「**セキュリティ**」タブをクリックし、「**Authenticated Users**」をクリックして、「**Authenticated Users のアクセス許可**」オプションで「**登録 (Enroll)**」が選択されていることを確認します。

エンタープライズ証明機関の構成

エンタープライズ証明機関を構成して TPM ユーザー証明書を発行するには、以下の手順を実行します。

1. 証明機関を開きます。
2. コンソール・ツリーで、「**証明書テンプレート**」をクリックします。
3. 「**操作**」メニューから、「**新規**」 → 「**発行する証明書 (Certificate to Issue)**」をクリックします。
4. 「**TPM**」をクリックし、「**OK**」をクリックします。

クライアントからの証明書の適用

クライアントから証明書を適用するには、以下の手順を実行します。

1. イントラネットへ接続し、Internet Explorer を開始して、CA サービスがインストールされているサーバーの IP アドレスを入力します。
2. プロンプト・ウィンドウにドメイン・ユーザー名とパスワードを入力します。
3. 「**タスクの選択**」の「**証明書の要求**」をクリックします。
4. Web ページの下部にある「**証明書の要求の詳細設定**」をクリックします。
5. 「証明書の要求の詳細設定」ページで、以下の設定を変更します。
   - 「**証明書テンプレート**」ドロップダウン・リストから「**TPM ユーザー (TPM User)**」を選択します。
   - 「**CSP**」ドロップダウン・リストから「**ThinkVantage Client Security Solution CSP**」を選択します。
   - 「**エクスポート可能なキーとしてマークする**」が選択されていないことを確認します。
   - 「**送信**」をクリックし、プロセスに従います。
   - 「証明書は発行されました」ページで「**この証明書のインストール**」をクリックします。「インストールされた証明書」ページが表示されます。

2008 ThinkPad ノートブック・コンピューター・モデル (R400/R500/T400/T500/W500/X200/X301) での USB 指紋センサー付きキーボードの使用

Lenovo は、ThinkPad® ノートブック・コンピューター・モデルと USB キーボードにおける指紋認証を提供する 2 つのベンダーと契約しています。2008 より前の ThinkPad ノートブック・コンピューター・モデル (例えば、T61 など) では、ThinkVantage 指紋センサーを使用します。2008 ThinkPad ノートブック・コンピューター・モデル (T400 以降) では、Lenovo 指紋センサーを使用します。Lenovo の USB 指紋センサー付きキーボードではすべて、ThinkVantage 指紋センサーを使用します。一部の ThinkPad ノートブック・モデル (例えば、外部 USB キーボードを備えた ThinkPad T400 など) で指紋センサー付きキーボードを使用するときには、特別な考慮が必要です。

このセクションでは、最新の ThinkPad ノートブック・コンピューター・モデルにインストールされた指紋認証ソフトウェアの一般的な使用法のシナリオとデプロイメントの戦略について説明します。

注:

- Lenovo Fingerprint Software

  Lenovo Fingerprint Software は、AuthenTec 指紋センサー (例えば、T400 内蔵の指紋センサーなど) のソフトウェアです。
- ThinkVantage 指紋認証ソフトウェア

  ThinkVantage 指紋認証ソフトウェアは、UPEK 指紋センサー (例えば、T61 内蔵の指紋センサー、すべての外部 USB キーボードの指紋センサーなど) のソフトウェアです。

Windows 7 のログオン

Windows 7 オペレーティング・システムにログオンするときには、随時、AuthenTec 指紋センサーも UPEK 指紋センサーも使用できます。

1. Lenovo Fingerprint Software バージョン 3.2.0.275 以降をインストールします。
2. ThinkVantage 指紋認証ソフトウェア バージョン 5.8.2.4824 以降をインストールします。
3. コンピューターを再起動します。指紋登録ウィザードが自動的に開始されます。
4. ThinkVantage 指紋認証ソフトウェアを使用して、外部指紋センサーに指紋を登録します。自動的に開始されない場合は、「**スタート**」→「**プログラム**」(または「**すべてのプログラム**」) →「**ThinkVantage**」→「**ThinkVantage 指紋認証ソフトウェア**」をクリックして、登録を開始します。
5. Windows パスワードを入力するように求められたら入力し、登録する指を選択します。
6. コンピューター画面のプロンプトに従い、外部指紋センサーを使用して指を登録します。
7. ウィンドウの上部にある「**設定**」をクリックします。

8. 「**Windows にログインするとき、パスワードではなく指紋スキャンを使用する**」チェック・ボックスを選択し、「**OK**」をクリックしてから、「**閉じる**」をクリックしてウィンドウを閉じます。
9. コンピューターを再起動し、外部指紋センサーで Windows にログオンするために指紋を使用できることを確認します。
10. 指紋の登録を使用して、内蔵指紋センサーで指紋を登録します。自動的に開始されない場合は、「**スタート**」→「**プログラム**」(または「**すべてのプログラム**」) →「**ThinkVantage**」→「**Lenovo Fingerprint Software**」をクリックして、登録を開始します。
11. Windows パスワードを入力するように求められたら入力し、登録する指を選択します。
12. コンピューター画面のプロンプトに従い、内蔵指紋センサーを使用して指を登録します。
13. ウィンドウの上部にある「**設定**」をクリックします。
14. 「**Windows にログインするとき、パスワードではなく指紋スキャンを使用する**」チェック・ボックスを選択し、「**OK**」をクリックしてから、「**閉じる**」をクリックしてウィンドウを閉じます。
15. コンピューターを再起動し、内蔵指紋センサーで Windows にログオンするために指紋を使用できることを確認します。

Client Security Solution と Password Manager

Windows ログオンとは異なり、Client Security Solution と Password Manager からの認証要求は、優先指紋センサーでのみ機能します。例えば、指紋センサー付きキーボードが接続されている場合、その指紋センサーが優先デバイスになります。指紋センサー付きキーボードが接続されていない場合は、ThinkPad 内蔵指紋センサーが優先デバイスになります。

優先デバイスを変更するには、次のようなレジストリー項目を作成します。

```
[HKLM¥Software¥Lenovo¥TVT Common¥Client Security Solution]
REG_DWORD "PreferInternalFPSensor" = 1
```

表 32. レジストリー・キー

名前	値	説明
PreferInternalFPSensor	0 (デフォルト)	指紋センサー付きキーボードが接続されているときには必ず、外部指紋センサーが優先されるように指定します。
	1	内蔵指紋センサーが優先されるように指定します。

プリブート認証 - BIOS パスワードの代わりに指紋を使用する

Windows ログオンとは異なり、BIOS パスワードの認証要求は、BIOS が使用されるように構成されているときにのみ、指紋センサーで機能します。デフォルトでは、BIOS は、指紋センサー付きキーボードが接続されている場合、そのキーボード

による指紋の読み取りを認識します。指紋センサー付きキーボードが接続されていない場合、BIOS は、内蔵指紋センサー・デバイスでの指紋読み取りを認証に使用します。

外部指紋センサー付きキーボードが接続されているときでも、**Reader Priority** の BIOS 設定を、内蔵指紋センサーを強制的に使用するように変更できます。**Reader Priority** のデフォルト値は「**External**」です。設定を「**Internal Only**」に変更して、内蔵指紋センサーを強制的に使用することができます。

注: この BIOS 設定は、BIOS 上の指紋プロンプトのみに適用されます。Windows ログオンや Client Security Solution の指紋認証要求には影響しません。

プリブート認証を使用可能にするための指紋認証ソフトウェアの構成

BIOS でスーパーバイザー、パワーオン、またはハードディスク・ドライブ・パスワードを設定した場合は、これらのパスワードを入力する代わりに、認証に指紋認証ソフトウェアを使用するように構成できます。

Lenovo Fingerprint Software - 内蔵指紋センサーの場合:

1. 「**スタート**」→「**プログラム**」(または「**すべてのプログラム**」) →「**ThinkVantage**」→「**Lenovo Fingerprint Software**」をクリックして、Lenovo Fingerprint Software を開始します。
2. 指紋を読み取らせるか、または Windows パスワードを入力するように求められたら、パスワードを入力します。
3. ウィンドウの上部にある「**設定**」をクリックします。
4. 「**パワーオンセキュリティとハードディスクのパスワードではなく指紋スキャンを使用する**」チェック・ボックスと「**パワーオンセキュリティのオプションを常に表示する**」チェック・ボックスを選択します。
5. 「**OK**」をクリックして、ウィンドウを閉じます。
6. 登録された指紋の 1 つを選択して、指紋を使用可能に設定し、BIOS パスワードを置き換えます。
7. 「**閉じる**」をクリックして、ウィンドウを閉じます。

ThinkVantage 指紋認証ソフトウェア - 外部指紋センサーの場合:

1. 以下のいずれかの方法で、指紋認証ソフトウェアを開始します。
   - 「**スタート**」 → 「**プログラム**」(または「**すべてのプログラム**」) → 「**ThinkVantage**」 → 「**ThinkVantage 指紋認証ソフトウェア**」をクリックします。
   - 「Lenovo ThinkVantage Tools」ウィンドウで、「**ThinkVantage 指紋認証ソフトウェア**」アイコンをクリックします。
2. 指紋を読み取らせるか、または Windows パスワードを入力するように求められたら、パスワードを入力します。
3. ウィンドウの上部にある「**設定**」をクリックします。
4. 「**パワーオンセキュリティとハードディスクのパスワードではなく指紋スキャンを使用する**」チェック・ボックスと「**パワーオンセキュリティのオプションを常に表示する**」チェック・ボックスを選択します。
5. 「**OK**」をクリックして、ウィンドウを閉じます。

6. 登録された指紋の 1 つを選択して、指紋を使用可能に設定し、BIOS パスワードを置き換えます。
7. 「**閉じる**」をクリックして、ウィンドウを閉じます。

付録 A. ThinkPad ノートブック・モデルで Lenovo 指紋センサー付きキーボードを使用する際の特別な考慮事項

一部の ThinkPad ノートブック・モデルで使用する指紋センサー・デバイスは、Lenovo 指紋センサー付きキーボードで使用する指紋センサー・デバイスと異なります。一部の ThinkPad ノートブック・モデルで指紋センサー付きキーボードを使用するときには、特別な考慮が必要となる可能性があります。

詳細については、Lenovo Web サイトにある指紋認証ソフトウェア・ダウンロード・ページにアクセスしてください。該当する ThinkPad ノートブック・モデルがリストされています。

指紋センサー付きキーボードと共に使用するときに特別な考慮が必要なのは、「Lenovo Fingerprint Software」の欄にリストされているモデルのみです。「ThinkVantage 指紋認証ソフトウェア」を使用する他のすべての ThinkPad ノートブック・モデルは、指紋センサー付きキーボードに組み込まれているデバイスと互換性のある指紋センサー・デバイスを使用し、特別な考慮は必要ありません。

設定とセットアップ

Lenovo Fingerprint Software 2.0 以降は、ThinkPad ノートブックで使用する指紋センサー・デバイスと共に使用できるようにインストールする必要があります。ユーザーは、内蔵されている指紋センサー・デバイスを使用して、Lenovo Fingerprint Software に指紋を登録する必要があります。

ThinkVantage 指紋認証ソフトウェア 5.8 以降は、Lenovo Fingerprint Keyboard と共に使用できるようにインストールする必要があります。ユーザーは、その指紋センサー付きキーボードを使用して、ThinkVantage 指紋認証ソフトウェアに指紋を登録する必要があります。

注: 1 つのデバイスに登録された指紋を、他のデバイスと交換することはできません。

ワークスペース認証

ワークスペース認証には、標準装備の指紋センサー・デバイスまたは指紋センサー付きキーボードが使用されます (システム電源をオンにする際のパスワードまたはハードディスク・ドライブのパスワードが指紋認証に置き換わります)。システムの電源がオンになると、使用するデバイスが BIOS によって決定されます。

デフォルトでは、BIOS は、指紋センサー付きキーボードが接続されている場合、そのキーボードによる指紋の読み取りのみを受け入れます。ワークスペース認証の場合、指紋センサー付きキーボードが接続されているときには、内蔵されている指紋センサー・デバイスによる指紋の読み取りは無視されます。指紋センサー付きキーボードが接続されていない場合は、ワークスペース認証に、内蔵されている指紋センサー・デバイスが使用されます。

「Reader Priority」の BIOS 設定を、標準装備の指紋センサーを使用するように変更できます。「Reader Priority」が「Internal Only」に設定されている場合は、ワークスペース認証に、内蔵されている指紋センサーを使用できます。この場合は、指紋センサー付きキーボードによる指紋の読み取りは無視されます。

Windows のログオン

Lenovo 指紋センサー付きキーボードおよび ThinkPad ノートブック・コンピューター・モデルで使用される指紋センサー・デバイスは、登録された指紋で Windows にログインするためのインターフェースをそれぞれ独自に備えています。

重要: 指紋ログオン・インターフェースが正しく構成されていない場合は、Windows のログオン・プロセスで互換性の問題が生じる可能性があります。

ThinkPad ノートブック・コンピューター・モデルが Lenovo 指紋センサー付きキーボードと内蔵の指紋センサー・デバイスの両方を装備し、かつ Client Security Solution がインストールされている場合、指紋認証を使用して Windows 7 オペレーティング・システムにログインするには以下の 2 つの方法があります。

- 指紋認証ソフトウェアのログオン・インターフェースを使用する

  Lenovo Fingerprint Software と ThinkVantage 指紋認証ソフトウェアの両方のログオン・インターフェースが使用可能でなければなりません。Windows 7 オペレーティング・システムで両方の指紋ログオン・インターフェースが使用可能になっている場合は、ユーザーが、指紋センサー付きキーボードと内蔵されている指紋センサー・デバイスのどちらかで指紋を読み取らせて、ログインできます。
- Client Security Solution のログオン・インターフェースを使用する

  指紋認証ソフトウェアのログオン・インターフェースの代わりに Client Security Solution のログオン・インターフェースを使用できます。Client Security Solution のログオン・インターフェースを使用して指紋認証により Windows オペレーティング・システムにログインする場合、それぞれの指紋認証ソフトウェアのワークスペースの「**設定**」オプションで指紋認証ソフトウェア・ログオンを使用不可にしてから、Client Security Solution の「**拡張**」メニューの「**セキュリティー・ポリシーの管理**」オプションで Client Security Solution のログオン・インターフェースを構成します。

  注:

  1. BIOS の「Reader Priority」設定は、この状態では適用されません。両方のデバイスが使用可能になっているときには、どちらかのデバイスをログオンに使用できます。
  2. Client Security Solution 8.3 以降のみがこの機能をサポートしています。詳しくは、『Client Security Solution での認証』を参照してください。

Client Security Solution での認証

注: 次の情報は、Client Security Solution 8.3 以降のみに適用されます。Client Security Solution の従来のバージョンでは、内蔵されている指紋センサー・デバイスと指紋センサー付きキーボードとの併用はサポートされていませんでした。

Client Security Solution を使用して指紋認証が必要なアクションを実行するときには (例えば、Password Manager を使用して Web サイトにパスワードを自動入力する場合など)、ユーザーは、指紋センサー付きキーボードが接続されていたら、指紋を求められたときに指紋を読み取らせる必要があります。指紋センサー付きキーボードが接続されているときには、標準装備の指紋センサー・デバイスによる指紋の読み取りは無視されます。指紋センサー付きキーボードが接続されていない場合は、内蔵されている指紋センサーを使用する必要があります。

Client Security Solution での認証に標準装備の指紋センサーを使用するようにユーザーに求めるには、レジストリー設定を使用できます。このレジストリー項目が設定された場合は、Client Security Solution での指紋認証を標準装備のセンサーで行なう必要があり、指紋センサー付きキーボードからの指紋の読み取りは無視されます。

レジストリー項目は次のとおりです。

```
[HKLM¥Software¥Lenovo¥TVT Common¥Client Security Solution]
REG_DWORD "PreferInternalFPSensor" = 1
```

Client Security Solution での指紋認証を標準装備のセンサーで行なう必要があるとき、上記のレジストリー項目のデフォルト値は 0 で、指紋センサー付きキーボードからの指紋の読み取りは無視されます。

この設定は、Client Security Solution の Administrative Template ファイルを Active Directory のグループ・ポリシーと共に使用して、変更することもできます。

注:

1. BIOS の「Reader Priority」設定が「**Internal only**」に設定されている場合、レジストリー項目値を 1 に設定することをお勧めします。これにより、Client Security Solution での認証で、BIOS ワークスペース認証の設定をシミュレートできるようになります。
2. BIOS 設定とこのレジストリー設定は独立しています。

付録 B. Windows パスワードのリセット後に Client Security Solution でパスワードを同期化する

Windows パスワードがリセットされた後、Client Security Solution によって、新しい Windows パスワードを入力するように連続して求められますが、パスワードが誤っていることを示すエラー・メッセージが表示されます。Windows セキュリティーはこのような方法で設計されているので、Windows パスワードがリセットされると、セキュリティー・クレデンシャルが無効になります。パスワードをリセットしようとするたびに、Windows から警告メッセージが出されます。また、Windows パスワードのリセットの影響を受けるのは Client Security Solution のみではなく、Windows EFS によって暗号化された証明書とファイルへのアクセスも失われます。Client Security Solution が (パスワードをリセットした結果として) Windows セキュリティー・クレデンシャルにアクセスできなくなると、Client Security Solution は新しいパスワードを入力するように連続して求め、入力されたパスワードが無効であることを示すエラー・メッセージを表示します。Windows セキュリティー・クレデンシャルがこの方法で無効になると、Client Security Solution は機能できなくなります。Windows パスワードが変更されたら (例えば、旧パスワードと新パスワードの両方を指定するように求められた場合など)、新しいパスワードによってセキュリティー・クレデンシャルが保存され、保護されます。

Windows パスワードのリセット後に CSS でパスワードを同期化するには、次のようにします。

1. Windows パスワードをリセットする前にシステムのバックアップを復元します。
2. Windows パスワードを元のパスワードにリセットします。これにより、Windows セキュリティー・クレデンシャルへのアクセスが復元されます。
3. 新規 Windows アカウントを作成し、破損したクレデンシャルを使用した元のアカウントではなく、新規アカウントの使用を開始します。
4. 次の方法に従って、システムをリカバリーします。
   a. Password Manager を起動します。
   b. 「**インポート/エクスポート**」をクリックし、「**項目リストのエクスポート**」を選択します。
   c. ファイルを保存する場所を指定し、ファイル名を入力します。
   d. 項目ファイルのパスワードを入力します。
   e. Password Manager を閉じます。
   f. Client Security Solution を起動します。
   g. 「**拡張**」→「**セキュリティー設定の再構成**」をクリックします。
   h. 新しい Windows パスワードを入力するように求められたら、パスワードを入力します。
   i. Client Security Solution から、システムを再起動するように求められます。
   j. システムが再起動したら、Password Manager を起動します。

k. 「**インポート/エクスポート**」をクリックし、「**項目リストのインポート**」を選択します。

l. 以前に保存したファイルを参照します。

m. パスワードを入力するように求められたら、入力します。

付録 C. 再インストールされた Windows オペレーティング・システムにおける Client Security Solution の使用

Client Security Solution がインストールされている Windows オペレーティング・システムを再インストールした場合、その新しくインストールした Windows オペレーティング・システム上で Client Security Solution を使用するには、Client Security Solution のインストール・データを消去してから、Client Security Solution を再インストールする必要があります。

そのためのベスト・プラクティスは、次のとおりです。

1. 現行の Windows オペレーティング・システムから Client Security Solution をアンインストールします。
2. コンピューターを再起動します。
3. レジストリーで以下のデータを消去します。
   - [HKEY_LOCAL_MACHINE¥SOFTWARE¥Lenovo¥TVT Common¥Client Security Solution]
   - [HKEY_LOCAL_MACHINE¥SOFTWARE¥Lenovo¥Client Security Solution]
   - [HKEY_LOCAL_MACHINE¥SOFTWARE¥Lenovo¥Logs]
   - [HKEY_LOCAL_MACHINE¥SOFTWARE¥IBM¥Security¥Debug]
4. C パーティションにある Client Security Solution に関連したデータを消去します。「フォルダ オプション」ウィンドウのすべての隠しファイルを表示するためのオプションを有効にして、C パーティション全体でデータを検索することをお勧めします。その結果、以下の場所に見つかる可能性があります。ただし、これ以外の場合もあります。
   - C:¥Users¥All Users¥Application Data¥Roaming¥Client Security Solution
   - C:¥Users¥%USER%¥AppData¥Roaming¥Lenovo¥Client Security Solution
5. BIOS Setup Utility でセキュリティー・チップをクリアしてから、以下を実行してセキュリティー・チップをアクティブにします。
   a. コンピューターをシャットダウンします。
   b. コンピューターの電源を入れ、F1 を押して BIOS Setup Utility に入ります。
   c. 「**Security**」を選択します。
   d. Enter を押して、「**Clear Security Chip**」を選択します。
   e. Enter を押して、「**Yes**」を選択し、暗号鍵を消去します。
   f. 「**Security Chip**」を選択してから Enter を押して、「**Active**」を選択します。

      注: Client Security Solution をハードウェア TPM モードに設定しない場合には、セキュリティー・チップを「**Disabled**」に設定します。
6. コンピューターを再起動し、Client Security Solution を再インストールします。

注: Client Security Solution インストール・モードをソフトウェア・エミュレーション・モードからハードウェア TPM ベース・モードに変更した場合、またはセキュ

リティー・チップをクリアした後、Client Security Solution は TPM の変更を検出すると既存のデータをリカバリーしようとしますが、暗号化データは新しい TPM データによって暗号化解除できないので失敗します。この場合、 Client Security Solution は起動できません。

付録 D. 特記事項

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、レノボ・ジャパンの営業担当員にお尋ねください。本書で Lenovo 製品、プログラム、またはサービスに言及していても、その Lenovo 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、Lenovo の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、Lenovo 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

Lenovo は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

Intellectual Property Licensing
Lenovo Group Ltd.
1009 Think Place
Building One
Morrisville, NC 27560
USA
Attention: Dennis McBride

Lenovo およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。 Lenovo は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書で説明される製品は、誤動作により人的な傷害または死亡を招く可能性のある移植またはその他の生命維持アプリケーションで使用されることを意図していません。本書に記載される情報が、Lenovo 製品仕様または保証に影響を与える、またはこれらを変更することはありません。本書におけるいかなる記述も、Lenovo あるいは第三者の知的所有権に基づく明示または黙示の使用許諾と補償を意味するものではありません。本書に記載されるすべての情報は、特定の環境において得られたものであり、例として提示されます。他の操作環境で得られた結果は、異なる可能性があります。

Lenovo は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本書において Lenovo 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この Lenovo 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性がありますが、その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

商標

以下は、Lenovo Corporation の商標です。

Lenovo
Rescue and Recovery
ThinkCentre
ThinkPad
ThinkVantage

IBM は、International Business Machines Corporation の米国およびその他の国における商標または登録商標です。

Microsoft、Internet Explorer、Windows Server、および Windows は、Microsoft グループの商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

用語集

暗号化システム (Cryptography system). 暗号化システムは、データの暗号化と復号の両方を行う単一の鍵を使用する対称鍵暗号化と、2 つの鍵 (全員に知られている公開鍵と鍵ペアの所有者のみがアクセス権を持つ秘密鍵) を使用する公開鍵暗号化に、大きく分類される。

エンベデッド・セキュリティー・チップ. エンベデッド・セキュリティー・チップは、TPM の別名。

管理者 (ThinkCentre)/スーパーバイザー (ThinkPad) BIOS パスワード. 管理者パスワードまたはスーパーバイザー・パスワードは、BIOS 設定を変更する能力を制御するために使用される。これには、エンベデッド・セキュリティー・チップを使用可能または使用不可にして、TPM 内に保存されたストレージ・ルート鍵をクリアする機能が含まれる。

公開鍵/非対称鍵暗号化 (Public-key/Asymmetric-key encryption). 公開鍵アルゴリズムは通常、2 つの関連した鍵のペアを使用する。1 つは秘密に保持されなければならない秘密鍵で、もう一方は公開される鍵で広く配布される。鍵が 1 つあった場合、ペアのもう一方が推測できるようであってはならない。「公開鍵暗号化」という用語は、鍵の一部を公開情報にするというアイデアから得られる。すべてのパーティーが同じ情報を保持しないことから、非対称鍵暗号化という用語も使用される。ある意味では、1 つの鍵がロック (暗号) を「ロック」し、別の鍵はそれをアンロック (復号) することを要求される。

ストレージ・ルート鍵 (SRK). ストレージ・ルート鍵 (SRK) は 2,048 ビット (あるいはそれ以上) の公開鍵ペア。これは最初は空で、TPM 所有者が割り当てられたときに作成される。この鍵ペアは、エンベデッド・セキュリティー・チップをそのままでは放置しない。 TPM の外部にあるストレージの秘密鍵を暗号化 (ラップ) し、TPM にロード・バックされたときにそれらを復号する。 SRK は、BIOS にアクセスのある人なら誰でもクリアすることができる。

対称鍵暗号化 (Symmetric-key encryption). 対称鍵暗号化暗号はデータの暗号化と復号に同じ鍵を使用する。対称鍵暗号は簡単で高速だが、主な欠点は、2 つのパーティーが何らかのセキュアな方法で鍵を交換しなければならないことにある。公開鍵暗号化は、公開鍵は非セキュアな方法で配布可能であり、秘密鍵は転送されることがないので、この問題を回避している。 Advanced Encryption Standard は対称鍵の一例。

Advanced Encryption Standard (AES). *Advanced Encryption Standard* は対称鍵暗号化技法。アメリカ政府は、それまで使用していた DES 暗号化に置き換えて、このアルゴリズムをその暗号化技法として 2000 年 10 月に採用。 AES は、凶暴なアタックに対して 56 ビット DES キーよりも高度のセキュリティーを提供する。また AES では、必要に応じて 128、192 および 256 ビット・キーの使用が可能。

TPM (Trusted Platform Module). TPM は特別な目的を持ってシステム内にビルドされた集積回路で、強力なユーザー認証とマシン検査を可能にする。 TPM の主な目的は、機密情報への不適切なアクセスを防止することにある。 TPM はハードウェア・ベースの信頼の基幹機能で、システム上のさまざまな暗号サービスを提供するように活用することができる。 TPM の別名はエンベデッド・セキュリティー・チップ。